Akin®

New York Department of Financial Services Issues Millions of Dollars in Penalties, Signaling Increased Cybersecurity Enforcement

Apr 26, 2021

Reading Time : **7 min**

By: Natasha G. Kohne, Erica Holland-Nesfield

April 14, 2021, Settlement

National Securities is a brokerage and insurance firm headquartered in New York and licensed by DFS to sell insurance, making it subject to the Cybersecurity Regulation. In compliance with the regulation, the firm reported two separate Cybersecurity Events that occurred in 2019 and 2020, both involving email accounts that lacked Multi-Factor Authentication (MFA) or alternative controls attacked through a phishing scheme. Both incidents potentially impacted customers' nonpublic information (NPI).

During the investigation into these reported events, National Securities informed DFS of two additional Cybersecurity Events that occurred in 2018 and 2019. National Securities reported the 2018 event to the Attorney General's Offices of New York, New Jersey, Connecticut and Massachusetts, notified all impacted customers, changed account credentials and provided credit monitoring to impacted customers. National Securities also notified impacted customers of the 2019 event, changed account credentials, provided credit monitoring to impacted customers and reported it to the Internal Revenue Service (IRS), Securities and Exchange Commission (SEC), Federal Bureau of Investigation (FBI) and the local County Sherriff's Office. However, the firm did not report either incident "as promptly as possible and no later than 72 hours of their occurrence" to DFS as required under the Cybersecurity Regulation.

The unreported events exposed NPI of certain customers through compromised Microsoft Office 365 email accounts of an employee and an independent contractor who is a broker at

a firm affiliate. National Securities investigation determined the email accounts were likely compromised by a phishing scheme. As a result of the unreported events, DFS found the following violations:

- **Section 500.12 Multi-Factor Authentication**
    - Failure to implement MFA or a reasonably equivalent or more secure access control for accessing the firm's email for all users until August 14, 2020. 500.12(b)
    - Failure to fully implement MFA for certain third party applications used by the firm which accessed the firm's internal network and consumer NPI. 500.12(b)
- **Section 500.17 Notices to Superintendent**
    - Failure to timely notify the DFS of two cyber events that occurred in April 2018 and March 2019. § 500.17(a)
    - Falsely certifying compliance for the calendar year 2018, where the firm timely filed Certification of Compliance but failed to comply with the MFA and breach notification requirements for the unreported events. 500.17(b)

In issuing a settlement, DFS acknowledged National Securities' "commendable cooperation" with the investigation and "recognize[d] and credit[ed]" the firm's ongoing efforts to remediate issues. In addition to the $3 million penalty, the largest published fine to date under the Cybersecurity Regulation, the Consent Order requires the firm to do the following within 120 days of the Order:

- Submit a **Cybersecurity Incident Response Plan** consistent with 500.16.
- Submit a **Cybersecurity Risk Assessment** of its information systems consistent with 500.09.
- Submit **Training and Monitoring** materials consistent with § 500.14.

Notably, DFS agrees in the settlement to take no further action against the firm for conduct in connection with its investigation, including MFA implementation issues through December 2020, reserving its right to take additional action in the future if it identifies any improper conduct not disclosed in the written materials submitted in connection with its investigation.

March 10, 2021, Amended Charges and Notice of Hearing

On March 10, 2021, DFS issued an Amended Statement of Charges and Notice of Hearing against First American Title Insurance Company ("First American"), the Nebraska-based stock insurance company subject to the first enforcement action under the Cybersecurity

Regulation by the DFS. Originally issued in July 2020, the charges were amended to include allegations regarding deficiencies in First American's vulnerability management program and deficiencies in qualifications of key personnel.

DFS now alleges that First American's vulnerability management program suffered from gross deficiencies in governance and inadequate methods to classify and respond to vulnerabilities. Although First American formalized a detailed policy and standard governing vulnerability management, DFS alleges the company failed to adhere to the policy and failed to remediate outstanding vulnerabilities. DFS alleges this failure created a backlog of unremediated vulnerabilities that grew over the years that contributed to the length of time a vulnerability existed, exposing millions of documents containing NPI to potential malicious actors.

DFS also added new allegations that key security personnel were not qualified to oversee important cybersecurity functions. Pointing to sworn statements, DFS alleges that a senior director of information security who managed the vulnerability management program admitted he lacked "technical expertise." According to the new allegations, in February 2020, one month after this individual testified that he "managed a data entry team" and had "no technical skills relating to cybersecurity" he was promoted to vice president with expanded responsibilities encompassing vulnerability management, application security and security operations, "key cybersecurity functions that require skills beyond managing data entry."

DFS added seven new charges describing the failures and violations as listed below:

- **Section 500.02 Cybersecurity Program**
    - Failure to maintain a cybersecurity program designed to perform certain "core cybersecurity functions" where it failed to implement a fully functional vulnerability management program in violation of § 500.02(b)(2).
- **Section 500.03 Cybersecurity Policy**
    - Failure to implement and maintain a written policy that addresses "systems and network security" where it failed to address the "voluminous amount of vulnerabilities" present in its Information Systems that went unremediated past deadlines set in company policies in violation of § 500.03(g).
- **Section 500.04 Chief Information Security Officer (CISO)**
    - Failure of the CISO to apprise the board of directors of the "deeply flawed state" of the company's vulnerability management where reports to the board

did not include the scope and nature of deficiencies, in violation of § 500.04(b).

- **Section 500.10 Cybersecurity Personnel and Intelligence**
    - Failure to "utilize qualified cybersecurity personnel" and provide "training sufficient to address relevant cybersecurity risks" where senior personnel managing cybersecurity program lacked requisite qualifications and training was insufficient to address relevant issues, in violation of § 500.10(a)(1) & (2).
- **Section 500.17 Notices to Superintendent**
    - Falsely certifying compliance for 2017 where it was aware of material deficiencies in its cybersecurity program at the time it certified, in violation of § 500.17(b).
    - Falsely certifying compliance for 2018 where it was aware of material deficiencies in its cybersecurity program at the time it certified, in violation of § 500.17(b).
    - Falsely certifying compliance for 2019 where it was aware of material deficiencies in its cybersecurity program at the time it certified, in violation of § 500.17(b).

The charges against First American are pending, a new hearing date is set for August 16, 2021.

March 3, 2021, Settlement

On March 3, 2021, DFS announced that Residential Mortgage Services, Inc. (RMS) agreed to pay a $1.5 million penalty for violations of the Cybersecurity Regulation to settle an enforcement action against the company. The Maine-based mortgage banker is licensed by DFS and subject to the Cybersecurity Regulation.

The enforcement action stems from the company's failure to disclose and investigate a 2019 data breach. RMS disclosed the breach 18 months after such breach when DFS conducted a safety and soundness examination in 2020, which included the company's compliance with the Cybersecurity Regulation. The breach involved unauthorized access to the email account of an employee who had access to a "significant amount of sensitive personal data" of customers. The intrusion occurred when the employee provided her employee email credentials in response to a phishing email that appeared to come from a business partner. RMS had implemented MFA, so that the employee also had to give approval via the MFA application on her phone to allow access. The employee granted authorization by tapping her

phone screen four times in one day in response to an alert from the MFA application, but after a fifth prompt the next day, where she was not trying to access her own account, she notified the company. Although RMS staff were alerted to the incident and blocked the unauthorized IP address, DFS found the company's investigation inadequate since it did not investigate the consumer data exposed especially where the employee handled Social Security and bank account numbers.

DFS concluded RMS should have notified the impacted customers and appropriate government bodies and lacked a comprehensive cybersecurity risk assessment. The regulator acknowledged that RMS had cybersecurity measures in place, such as MFA for remote access through an authenticator device antivirus protection and end-point protection software and, but found RMS's risk assessment lacking as it **should have** led to the periodic evaluation of controls to protect NPI, information systems and result in a program tailored to safeguard the company's data. In addition to the $1.5 million penalty, DFS imposed a remediation plan on RMS. Within 90 days of the Order, RMS is required to:

- Submit a comprehensive **Cybersecurity Incident Response Plan** consistent with § 500.16.
- Submit a **Cybersecurity Risk Assessment** consistent with § 500.09.
- Submit **Training and Monitoring** materials consistent with § 500.14.

February and March 2021 Cybersecurity Alerts and Guidance

DFS issued two cybersecurity alerts and new guidance for insurers in the first quarter of the year as well. On February 4, 2021, DFS issued a new Cyber Insurance Risk Framework that outlines industry best practices for New York-regulated property/casualty insurers that write cyber insurance. On February 16, 2021, DFS issued a cybersecurity fraud alert regarding a widespread cybercrime campaign to steal consumers' NPI from public-facing websites that transmit or display redacted NPI. On March 9, 2021, DFS issued an alert regarding vulnerabilities in Microsoft Exchange Server, directing regulated entities to "immediately patch or disconnect vulnerable servers" and use tools identified by Microsoft to remediate the issue. The alert reminds regulated entities to report Cybersecurity Events pursuant to § 500.17(a).

With this recent activity, DFS begins to position itself as one of the leading state regulators in cybersecurity enforcement. These actions begin to develop a body of enforcement guidance that may be persuasive to other states and regulators. To read more about the Cybersecurity

Regulation and other cyber developments in the financial services industry, see our other posts here and here.

Categories

Financial Data Privacy | State Privacy Policy | Cybersecurity & Information Security