Effective Access Controls, Timely Breach Notification and Other Takeaways from the Latest NYDFS Cyber Resolution

April 15, 2021

On April 14, 2021, the New York State Department of Financial Services (the "DFS") announced that its cyber-enforcement action against National Securities Corporation ("National Securities") has been resolved by a Consent Order that imposes a $3 million penalty. This is the latest step in the DFS's very active cyber-enforcement agenda. The charges against First American Title Insurance Company are pending with an August 16 hearing date, and last month, the DFS reached its first full cybersecurity resolution with Residential Mortgage Services.

The resolution—the first cyber resolution on the insurance side of the DFS house—cites National Securities for several violations of the DFS Part 500 Cybersecurity Regulation ("Part 500"), including:

- Failure to implement multifactor authentication ("MFA"), or a reasonably equivalent security control, for accessing National Securities' email environment, leading to four breaches;
- Failure to notify the DFS of two of the cybersecurity events; and
- Falsely certifying compliance with Part 500.

In addition to the $3 million fine, National Securities must undertake various risk-mitigation measures in an effort to prevent future incidents.

National Securities' Reported Cybersecurity Events. National Securities is headquartered in New York and is licensed by the DFS to sell insurance, making it subject to Part 500. National Securities experienced two cybersecurity events that it reported to the DFS:

- In September 2019, National Securities discovered that an employee's email account, which lacked MFA or alternative controls as required by Part 500, had been compromised by what was likely a phishing scheme. This likely resulted in unauthorized access to certain customers' nonpublic information.

- In April 2020, National Securities discovered that the email account of a broker at one of National Securities' affiliates, which did not have MFA enabled, was successfully phished. Ultimately, National Securities determined that $400,000 of client funds were taken. The incident also potentially impacted some customers' nonpublic information.

National Securities' Unreported Cybersecurity Events. During its investigation into National Securities' cybersecurity program, the DFS became aware of two cyber incidents that National Securities had not reported to the DFS promptly:

- In April 2018, National Securities learned that a threat actor had set up an automatic forwarding rule on its CFO's email account, potentially exposing customers' nonpublic information. Although National Securities notified the Attorneys General of New York and several other states, National Securities failed to notify the DFS of that event.

- In March 2019, National Securities discovered a phishing scheme that granted an unauthorized threat actor access to an employee's secure document management system account. Again, although National Securities notified several federal agencies and local law enforcement, it did not notify the DFS.

Because of the violations mentioned above, the DFS also determined that National Securities falsely certified compliance with the MFA and breach notification requirements of Part 500.

Terms of the Settlement. In assessing the $3 million penalty, the DFS considered National Securities' cooperation, its ongoing efforts to remediate cybersecurity shortcomings and its commitment to devote significant financial resources to enhance the company's cybersecurity program. The other terms of the settlement include submission of the following to the DFS within 120 days:

- A comprehensive cybersecurity incident response plan;

- A cybersecurity risk assessment; and

- Training and monitoring documents demonstrating risk-based policies and procedures for monitoring users' activity and identifying unauthorized access and updated training based on the findings of the risk assessment.

KEY TAKEAWAYS

- The Need for MFA or Equivalent Approved by the CISO: Entities subject to Part 500 must implement MFA for all individuals who access the entity's internal networks from an external network, which includes contractors with remote access that is similar to employee access. National Securities appears to have implemented access controls designed to reduce the risks associated with some of its MFA gaps, but the DFS viewed those measures as insufficient. In the absence of MFA, such compensating controls can only satisfy the Section 500.12 requirements if the CISO has approved them, in writing, as providing reasonably equivalent protection.

- The Need to Notify the DFS Whenever Other Regulators Are Required to Be Notified of a Cybersecurity Event: Section 500.17(a)(1) of Part 500 provides that notification to the DFS is mandatory whenever a cybersecurity event (i) impacts a DFS-regulated entity and (ii) notice of that event is required to be provided to any government body, self regulatory agency or other supervisory body.

- Dealing Effectively with Obligations Around Third-Party Applications and Personnel: The DFS notes that there is an obligation under Part 500 to implement MFA for third-party applications, indicating that even as of the date of the Consent Order, National Securities had not fully met that obligation. The Consent Order also calls out National Securities for implementing MFA for certain employee users while taking an additional year to do the same for independent contractors with access to its internal network.

- The DFS Views Certifications as Requiring Full Compliance: The Consent Order provides that because of the MFA and breach notification failures, National Securities' annual certification of compliance to the DFS was false, and that was considered a separate violation of Part 500.

CONCLUSION

This Consent Order underscores the importance with which the DFS views Part 500's access-control requirements. The DFS is also making clear that, absent a compensating control, MFA is required for everyone who remotely accesses the network—employees and third parties alike. Regulated entities should carefully review their network access controls to ensure they have implemented MFA for anyone who can remotely access their network or that any compensating control has been approved by the CISO, in writing, as providing equivalent protection.

The DFS also makes clear that it expects full compliance with the Part 500.17(a) requirement to provide notice to the DFS when other regulators are being notified about a cybersecurity event. Regulated entities should review their incident response plans and playbooks to ensure that they are taking the Part 500.17(a) follow-on notice requirement—and its quick 72-hour window—into consideration when evaluating notification obligations. Even regulated entities that otherwise comply with their state or federal breach-notification obligations can be subject to an enforcement action for failure to notify the DFS as required.

* * *

Debevoise has developed the Debevoise Data Portal, an online tool to help companies quickly assess their federal, state and international breach-notification obligations resulting from a cyber incident. Please contact us at dataportal@debevoise.com for more information.

To subscribe to the Data Blog, please click here.

Please do not hesitate to contact us with any questions.

NEW YORK


Jeremy Feigelson
jfeigelson@debevoise.com


Avi Gesser
agesser@debevoise.com


Jim Pastore
jjpastore@debevoise.com


Johanna N. Skrzypczyk
jnskrzypczyk @debevoise.com


Parker C. Eudy
pceudy@debevoise.com


Christopher S. Ford
csford@debevoise.com


Mengyi Xu
mxu@debevoise.com

WASHINGTON, D.C.


Luke Dembosky
ldembosky@debevoise.com