First DFS Resolution Under Its Cyber Rules Highlights the Risks of Inadequate Cyber Investigations

March 8, 2021

Last year, we discussed the first enforcement action brought by the New York State Department of Financial Services ("DFS"), which involved charges against First American Title Insurance Company. That hearing is scheduled for March 22.

On March 3, 2021, the DFS reached its first full resolution under its Part 500 Cybersecurity Regulation, a Consent Order with Residential Mortgage Services that imposes a $1.5 million penalty for several violations including:

- Failure to investigate whether an attacker, who compromised a single email mailbox, accessed private data of individuals.
- Failure to satisfy various state breach notification obligations.
- Failure to notify the DFS of the incident.
- Failure to conduct a cybersecurity risk assessment, as required by Part 500.

In addition to the $1.5 million fine, Residential Mortgage must undertake various risk mitigation measures to prevent future incidents.

RESIDENTIAL MORTGAGE'S CYBERSECURITY EVENT

Residential Mortgage is headquartered in Maine and is licensed by the DFS as a mortgage banker, which is why it is subject to Part 500.

From March to August 2020, examiners from the DFS conducted a safety and soundness review, which included Part 500 compliance. In confirming that no cybersecurity events had been reported to the DFS during the review period, Residential Mortgage's CISO disclosed an email compromise that had occurred 18 months earlier. On March 5, 2019, the email account of an employee who collects significant amounts of personal data

from loan applicants—including social security numbers and bank account numbers—was compromised through a phishing email.

Soon after, Residential Mortgage determined that an attacker, with an IP address in South Africa, accessed the employee's email account on four separate occasions. Though Residential Mortgage had instituted multi-factor authentication ("MFA"), the targeted employee granted the requisite authorization by tapping her phone screen on four separate occasions, even though she had not been attempting to access her own email account. Upon receiving a fifth prompt on the following day, the employee notified the company, which then blocked further access by the attacker. After determining that the unauthorized access was limited to a single mailbox, no further investigation was conducted.

It was only after the issue was raised by the DFS that Residential Mortgage engaged a law firm to oversee a review of the contents of the mailbox and make the necessary regulatory notifications to state authorities and impacted customers, which included an offer for free credit monitoring and identity theft protection to impacted individuals.

It is unclear from the Consent Order whether the DFS took issue with the MFA program employed by Residential Mortgage, which required a screen tap when prompted. Such MFA tools may be viewed as not providing the same level of protection as those that require users to obtain and enter a one-time security code.

FAILURE TO CONDUCT A RISK ASSESSMENT

During the examination, the DFS also discovered that Residential Mortgage had not conducted a comprehensive risk assessment, as required by Part 500. Despite that failure, the company had filed its annual Certification of Compliance with Part 500 for the calendar year 2019.

TERMS OF THE SETTLEMENT

In assessing a $1.5M penalty, the DFS considered the cooperation of Residential Mortgage, its financial resources and good faith, and the gravity of the violation. The DFS also acknowledged the company's ongoing efforts to remediate the shortcomings identified in the Consent Order. The other terms of the settlement include submission of the following to the DFS within 90 days:

- A comprehensive cybersecurity incident response plan.

- A cybersecurity risk assessment.

- Certain training and monitoring documents.

FOUR TAKEAWAYS

- **The Need to Conduct a Reasonable Investigation of a Cyber Incident**: In its Statement of Charges against First American, the DFS stressed that, after the data exposure was discovered, the company failed to conduct a reasonable investigation into the scope and cause of the incident, thereby underestimating the seriousness of the vulnerability. Similarly, with Residential Mortgage, the DFS characterized the company's investigation of the cyber incident as "inadequate" because it did not review the contents of the compromised mailbox. The DFS viewed this as "especially egregious" given the employee's routine handling of private data of customers (including social security and bank account numbers) through her email.

- **The DFS Cares About Compliance With State Breach Notification Laws**: One of the two triggers for notification to the DFS of a cybersecurity event is an incident that requires notification to any other government agency. Accordingly, when a DFS-regulated entity fails to investigate an incident, and that failure results in missed notifications to state regulators, it also leads to a missed notification to the DFS.

- **The Need to Conduct a Risk Assessment**: Part 500 requires companies to conduct an annual risk assessment. The Consent Order with Residential Mortgage makes clear that the DFS views this as a critical component of Part 500 compliance. Indeed, the DFS viewed the company's failure to conduct a risk assessment as undermining the accuracy of its annual certification of compliance.

- **The Need for Appropriate Training**: The charges against First American included an alleged violation of the Part 500 training requirements—that entities conduct regular cybersecurity training for all personnel, and that the training reflect risks identified by the entity's risk assessments. Although the Residential Mortgage Consent Order does not have a specific finding with respect to training, the fact that it requires Residential Mortgage to submit its most recent cybersecurity training suggests that the DFS views employee training as an important part of a company's efforts to remediate following a finding of an inadequate investigation.

CONCLUSION

This Consent Order and the charges against First American demonstrate that the DFS regards Part 500 as creating substantive obligations for both business-as-usual and incident response, and that violations of those obligations can result in an enforcement action independently of whether any harm results from the lack of compliance.

From a cybersecurity point of view, the incident in Residential Mortgage may appear insignificant—the compromise of a single email account. But the Consent Order makes clear that the DFS views the severity of a cyber incident as dependent on the contents of the compromised data, not the just the volume, and therefore, a failure to conduct an adequate investigation into what was compromised may be viewed as a violation of Part 500. Accordingly, if a company has reason to believe that attackers have accessed an employee's mailbox, then the company should consider taking reasonable steps to determine whether any state breach notification obligations are triggered. This likely doesn't mean that every email in the inbox needs to be reviewed. Rather, depending on the circumstances, companies may be able to discharge their obligations to conduct a reasonable investigation by doing one or more of the following:

- Assessing whether the contents of the mailbox were accessed or acquired by the attacker.
- Interviewing the employee to assess the likelihood that there is sensitive personal information in the mailbox.
- Running targeted searches through the mailbox or using automated review tools to look for sensitive personal information.
- Reviewing a sample of emails from the mailbox.

Then, depending on the results of those inquiries, the company will have to assess whether addition investigatory steps are appropriate.

* * *

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

Avi Gesser
agesser@debevoise.com

James Pastore
jjpastore@debevoise.com

Christopher S. Ford
csford@debevoise.com

Alexandra N. Mogul
anmogul@debevoise.com

Sarah Q. Smith
sqsmith@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com