Cybersecurity Law Report
An Acuris company

Lowenstein Sandler

May 5, 2021

FINANCIAL SERVICES REGULATION

Two Settlements Show NYDFS' Hidden Power to Use Other States' Breach Laws

By Matt Fleischer-Black, *Cybersecurity Law Report*

The New York Department of Financial Services (NYDFS) has announced its first two consent orders addressing violations of its influential Cybersecurity Regulation (Regulation), imposing a total of $4.5 million in penalties. Both orders target companies' failure to notify NYDFS of security breaches. In each, NYDFS takes pains to highlight that the 2017 Regulation obliges a company to report all security incidents "impacting" it if any other governmental or self-regulatory authority requires notice — extending the New York arm of the law possibly around the globe.

"The agency is saying that if you have to notify anybody else, then you have to notify us, too," Lowenstein Sandler partner Mary Hildebrand told the Cybersecurity Law Report. This almost-royal power to use all other cybersecurity laws has been in plain sight, if easy to overlook: the same Regulation section imposes NYDFS' infamous 72-hour reporting deadline.

NYDFS' press releases for these settlements declare that it is taking "nation-leading actions" to protect customers across the country from its licensees' cybersecurity shortcomings. One punishment, against National Securities Corporation (National), carries harsh implications in an era of rampant ransomware. The order bars the company from using insurance proceeds to pay its penalty. "It's unusual. I don't remember seeing that before with cybersecurity," Hildebrand said.

The breaches addressed in the consent orders each involve phishing incidents. They lay bare the department's readiness to punish missteps around limited email compromises without evidence of actual harm.

The orders also highlight that NYDFS is policing companies' use of multi-factor authentication (MFA) with third-party applications and cloud platforms, and the regulator's willingness to hold companies accountable for compliance before the department started enforcement in 2020.

In this article, we discuss New York's expansive breach obligations, the perils of a pioneering punishment and the top compliance implications of both settlements with enforcement specialists from Alston & Bird, Hogan Lovells and Lowenstein Sandler.

See "Six Compliance Lessons From NYDFS' First Cybersecurity Regulation Enforcement Action" (Aug. 12, 2020).

Consent Order for National Securities Corporation

On April 14, 2021, NYDFS settled with National, a licensed insurer, for failing to provide timely notice to NYDFS of two cybersecurity events reported to other regulators, failing to properly implement multi-factor authentication (MFA), and for falsely certifying its compliance with the Regulation.

National agreed to pay a $3 million penalty, take several remedial steps and submit an incident response plan and risk assessment to NYDFS in four months. The $3 million penalty is to date the largest disclosed penalty for violations of the Regulation. (The department's July 2020 enforcement action against First American Title Insurance alleges more substantial violations of the Regulation, but the company will contest the charges at an August 21, 2021, hearing.)

Four Phishing Incidents but Only Two Notifications

National suffered at least four successful phishing attacks between 2018 and 2020. NYDFS said these attacks involved sensitive personal data and possibly affected thousands of New Yorkers and other members of the public.

NYDFS faulted National for not notifying it of two of these incidents. In April 2018, seven months after the Regulation went into effect, cyber criminals accessed the email account of its Chief Financial Officer and potentially accessed customers' non-public information (NPI). Then, in March 2019, attackers accessed a document management system in National's tax software.

National notified four state attorneys general of the April 2018 incident, according to the consent order. It reported the second breach to the IRS, SEC, FBI and a local sheriff. Both times it provided credit monitoring to potentially affected customers

National did notify NYDFS about two later incidents. In September 2019, the order says, cyber intruders accessed the company's network through an email account, which potentially affected customers' NPI. Then, in April 2020, a contractor at an affiliate firm noticed unauthorized fund transfers from client accounts. An email account had been compromised for six weeks, and the company lost $400,000. National provided credit monitoring to customers and refunded money.

See "What the New Information Security Reporting Standards Mean for Financial Institutions" (Feb. 5, 2021).

Violations of Notice and MFA Requirements

NYDFS said that National had not fully implemented MFA for all users until August 2020. The agency highlighted that National had over 60 third-party applications.

The regulator also said that National's CISO did not approve in writing the access controls that National used before implementing MFA. NYDFS deemed those controls insufficiently equivalent to MFA, as the Regulation requires.

National's insufficient implementation of access controls and its failure to notify NYDFS of the breaches resulted in it falsely certifying its compliance with the Regulation in 2018.

Settlement Terms

In addition to the monetary penalty, National must submit within four months a cybersecurity incident response plan and a comprehensive risk assessment. The company must also provide to NYDFS an update of its training materials that it uses with all employees to sharpen cybersecurity awareness, which must reflect the conclusions of its updated risk assessment.

NYDFS lauded National's "commendable cooperation" with the investigation and its effort to fix the issues, including its spending money and devoting resources to upgrade its cybersecurity. However, it prohibited the company from using any insurance payouts to cover the penalty.

Consent Order for Residential Mortgage Services

On March 3, 2021, NYDFS settled with Residential Mortgage Services (Residential), a licensed mortgage banker, contending that Residential had failed to adequately investigate a security breach, timely notify the department or affected consumers of it, and conduct a sufficient risk assessment.

Residential agreed to pay a $1.5 million penalty, take several remedial steps and submit an incident response plan and risk assessment to NYDFS in three months.

Phishing Hits Employee Handling Sensitive Loan Data

NYDFS examiners started a six-month safety and soundness review of Residential in March 2020. Midway through the review, Residential's CISO disclosed a March 2019 email compromise, in which an attacker eluded its MFA controls.

A Residential employee handling sensitive personal data from mortgage loan applicants clicked on a phishing email, purportedly from a business partner. When her smartphone flashed an MFA prompt, she tapped to allow access to her email account. That evening, she approved three more MFA requests. The next morning, she rejected the fifth MFA request and contacted the IT department.

Residential's IT team blocked the intruders, ostensibly from South Africa. The IT team found no trace of the intruders beyond the initial employee's email account, and left the matter there.

Violations for Investigation and Risk Assessment

The failure to investigate the breach further "was especially egregious given Employee's daily handling of the private data of mortgage loan customers," including bank account numbers, the consent order contends. NYDFS added that Residential failed to check whether the employee's mailbox held consumers' NPI, determine which customers the breach affected, and make applicable notifications.

NYDFS also deemed Residential's risk assessment inadequate. Because of these shortcomings, the CISO's Certification of Compliance for 2019 was inaccurate.

Settlement Terms

Beyond paying $1.5 million, Residential will submit an incident response plan, a cybersecurity risk assessment and updated training materials to NYDFS within 90 days. The consent order lauds Residential's "commendable cooperation," its dedication of money and resources to fixes and improvements, and its post-examination changes to "policies, procedures, systems, governance structures and personnel." Indicating that NDYFS intends the consent order as a message for its licensees, it praises a detailed list of access control and detection measures that Residential took before and after the 2019 incident.

The Orders' Implications

In the wake of these orders, most NYDFS licensees should review the company's incident response plan, risk assessment effort and latest employee training to ensure that each meets the Regulation's standards, said Hogan Lovells senior associate Jasmeet Ahuja. "NYDFS examinations have increased," she reported, so legal and compliance teams "should ensure that they are talking to their IT department or security operations center and are aware of all incidents, and that there's a coordinated effort to respond as NYDFS' regulation requires."

NYDFS Examines Past and Current Compliance

Companies should scrutinize their NYDFS Certifications of Compliance for inaccuracies and omissions of phishing episodes.

In the Residential and National orders, "the regulator looked at incidents going back to 2018 and 2019," when a compliance grace period was in effect. "NYDFS is assessing past compliance as well as current compliance," Alston & Bird counsel Michael Young cautioned.

See "How Is COVID-19 Affecting Cybersecurity Risk, Readiness, Reporting and NYDFS Enforcement?" (Apr. 22, 2020).

Multiple Triggers to Notify NYDFS

The Regulation (500.17) requires companies to notify NYDFS of a security incident within 72 hours, currently the most demanding requirement in the U.S. With this requirement and Europe's GDPR, "the 72-hour time frame has led to tremendous overreporting. Rather than face the consequences of missing the deadline," companies send in initial blips of trouble, said Hildebrand.

NYDFS' large punishments for failure to report modest compromises are sure to spur even more reports. Bankers like Residential face fines of $2,500 per day per violation, while insurers and other financial institutions face $1,000 per day.

The 72-hour burden and million-dollar punishments should not blind companies to the other demanding aspects of NYDFS notifications that these consent orders spotlight, Hildebrand cautioned.

In most other states, potential harm to individuals' PII triggers breach notification. New York's Regulation adds a second ground for reporting, when a breach threatens the integrity of the company's information systems or "the event has a reasonable likelihood of

materially harming any part of the operations of the company," Hildebrand noted.

To weigh whether an episode meets this vague reporting threshold, companies must involve lawyers in evaluating IT trouble at an early stage, Hildebrand advised.

Assessing the risk of a phishing incident requires tough judgments, as the Residential order demonstrates. How can companies determine the likelihood that an email compromise will cause business-wide material harm? Lawyers can start by asking about:

1. the exploit's scope and containment;
2. PII's potential presence in any affected accounts; and
3. whether attackers made downloads or screenshots.

NYDFS Leverages Laws Here, There and Everywhere

The third and broadest Regulation report trigger is notice to other authorities, including self-regulatory bodies. "Department licensees must notify DFS within 72 hours of a determination that a Cybersecurity Event requiring notice to another agency has occurred," the Residential consent order declares.

Both orders emphasize this. NYDFS counts off eight other authorities that National notified while leaving the New York regulator in the dark. The department says that Residential's phishing incident met the Regulation's standard for a direct 72-hour notification. Then, seemingly gratuitously, the order looks across borders, identifying three states that also deserved notice because the breach affected their residents – and highlights that notifying "another agency" compels an NYDFS report.

The Regulation's notification provision extends NYDFS' shadow across the cybersecurity landscape, Hildebrand observed. "It's clever. It is leveraging the other states' laws, and all their constant changes, without having to update their own law," she said. "Back in 2017, someone at the department foresaw how radically the data breach laws would change over the next several years to become far stricter than previously, to include additional categories of personal information, such as biometric and genetic data," she pointed out.

These orders suggest that "New York's first-in-the-nation Cybersecurity Regulation" (as the orders label it) puts NDYFS first in line for breach notification – before the local regulator. Other states have looser deadlines, like the common (and permissive) "when reasonably practicable." NYDFS declined to comment on this odd consequence of the Regulation.

NYDFS did not come down on National as hard as it could have over notification failings. With the two later breaches, the company took 35 and 12 days, respectively, to alert NYDFS, the consent order says. Yet, the order does not include a timely-notice violation for either incident.

Penalty Barring Use of Insurance Money

NYDFS' prohibition on using insurance to sidestep the penalty for a cybersecurity violation is eye-opening amidst the drumbeat of ransomware attacks. NYDFS investigators, responding to a covered entity's ransomware notice, are likely to uncover shortcomings in the entity's risk assessment or training – typically underfunded tasks that need constant attention. "This regulatory risk is part of why companies are getting cyber insurance in the

first place. Some policies will cover the penalties or payments," Ahuja said.

The insurer might issue a lump sum to cover a penalty together with other damage costs, so this punishment could complicate the company's discussions with its insurance adjuster, Hildebrand noted.

See "Steps to Take After OFAC and FinCEN's Warnings on Ransomware Payoffs" (Oct. 21, 2020).

Multi-Factor Authentication for Third Parties

The National consent order flagged the company's failure to fully implement MFA beyond its central all-employee computing environments. "It cited the fact that there were 60 third-party vendors involved with this entity that did not use two-factor authentication or a reasonable substitute for it," Hildebrand noted.

The Regulation requires MFA (or a CISO-approved substitute) when any employee or third party remotely accesses internal networks. The consent orders, Young said, "raise a question of whether companies now should treat MFA as being per se required any time they are using a third-party cloud application, for backend administrative support, for example," and the information resides on an external network.

See "Overcoming the Challenges and Reaping the Benefits of Multi-Factor Authentication in the Financial Sector (Part One of Two)" (Jul. 26, 2017); Part Two (Aug. 9, 2017).

Incident Response Plans Include Initial Incident Triage

Companies, like Residential, often conclude that a phishing incident does not trigger regulatory reporting because they found minimal harm to customer data or their network. These NYDFS orders, and earlier First American charges, suggest companies must ensure rigor in their initial triage evaluation of any security episode, Ahuja said.

Companies should detail in written procedures, Ahuja advised, "when there is a possible incident, and what happens next. Who needs to be notified to be in the loop?" This will address the Regulation mandate (500.16) to "codify" incident response processes.
A good approach, Ahuja explained, is to have a procedure directing the IT department to always alert the legal department immediately after determining whether a compromised email account or associated employee handles PII, even if no other information is known. Document this whole process, too, to help avoid NYDFS scorn for an "inadequate investigation."

Tabletop exercises help spot holes in plans, Ahuja pointed out. Companies can run limited exercises focused on the incident triage to check whether decisive legal questions are addressed to determine whether notice would be required.

See "Six Ways to Be Prepared for the SEC's Focus on Cybersecurity and Resiliency" (Apr. 15, 2020).

Updated Risk Assessments

Whether because of an incident or an examination, NYDFS is scrutinizing companies' "periodic" risk assessments, these orders show. After SolarWinds, Microsoft Exchange, ransomware and other evolving threats, and the disruption COVID-19 caused to regular processes, companies will need to update their risk assessments for NYDFS, Ahuja advised. One update that companies can do now is to

create a component of the assessment to "examine how to address one or a few of these new vulnerabilities," she advised.

Companies also must add in risk reports for technology changes of the past year, like application switches or integrations. These additions should address how to "ensure that the appropriate chain of people approve the new implementations," Ahuja noted.

A complete overhaul to the risk assessment may be appropriate in some instances. Certain companies may want to invest in a fresh assessment as a springboard to get beyond a mere checklist review, which likely will not suffice for NYDFS and other aggressive cybersecurity regulators, Young said. Paying consultants to test controls, weigh in on risks, or prompt a round of "self-examination, even if it is uncomfortable or expensive, is a good way to ensure your assessment actually informs your cybersecurity program," he observed.

"The Regulation imposes compliance costs on licensees," Young continued. Incident response plans, governance measures and risk assessments add up – but the Residential and National orders highlight the eventual financial savings. "With this strict enforcement and the increasing penalties, the NYDFS seems intent on making the cost of noncompliance higher than the cost of compliance," he said.

See "Implementing NSA-CISA-FBI Advisory Mitigation Tactics for Vulnerabilities Exploited by Russia" (Apr. 28, 2021).