PUBLICATION

NYDFS Surges Ahead with Cybersecurity Enforcement: Recent Fine Highlights Need for Financial Institutions to Focus on Incident Response

Authors: Matthew George White, Alexander Frank Koskey, III
March 08, 2021

The New York Department of Financial Services (NYDFS) has become a frequent topic of these alerts. In recent weeks we have covered multiple actions from the regulator, including its first enforcement action, its SolarWinds notification requirement, and its first-in-the-nation Cyber Insurance Risk Framework. NYDFS continues to push forward with enforcement of its Cybersecurity Regulation. On March 3, the regulator announced that it had fined a licensed mortgage banker $1.5 million for failing to report a cyber breach exposing private data of its customers. The settlement highlights the need for financial institutions to focus on their incident response programs, including developing a robust and comprehensive incident response plan, ensuring that the plan is activated when necessary, and testing and revising the plan to ensure the institution stands ready to respond to a data incident.

Summary of Allegations

NYDFS alleged that in March 2019, an email account of one of the mortgage banker's employees was compromised allowing a threat actor unauthorized access to a significant amount of personal information on the company's mortgage loan applicants. The employee regularly handled the private data of mortgage customers, including social security numbers and bank account numbers, via the breached email account. NYDFS alleged that the mortgage broker failed to report the incident to NYDFS and failed to conduct an investigation and identify the customer data exposed until prompted to do so by the regulator in September 2020, nearly 18 months after the incident. Accordingly, NYDFS determined that the company failed to comply with the Cybersecurity Regulation's requirements for timely reporting of the breach and having in place a comprehensive cybersecurity assessment.

The mortgage banker was fined $1.5 million despite the NYDFS's acknowledgment that the company cooperated throughout its investigation, committed to undertaking significant improvements to its cybersecurity program, and agreed to expedite remediation of its cyber controls.

Takeaways

On their face, business email compromises are fairly common and unremarkable incidents. In today's environment many businesses, including many financial institutions, are regularly targets of email account compromise attempts. Whether these attempts arise out of phishing, social engineering, or a variety of other common attack vectors, their effects can be substantial. While there are a variety of tools and processes organizations can utilize to mitigate these risks, it is virtually impossible for a business to completely insulate itself from these attacks. As such, it is vitally important that businesses implement robust risk assessment procedures to detect unauthorized access to sensitive and customer data, train employees to identify these attacks, and develop, test, and maintain a robust incident response program.

In particular, this incident highlights the need for organizations to focus on their incident response plans. With multiple known and common threats in the landscape, and a host of new and developing threats arising on a regular basis, organizations must develop and refine their incident response plans to address these threats. This also includes testing that plan through tabletop exercises and evaluating how to respond to varying

incidents. As the landscape of potential threats continues to grow, financial institutions must be proactive in taking steps to ensure that they are appropriately prepared to respond once an actual attack occurs.

In developing your incident response plan, critical considerations include:

- Who is part of your response team? Do you have representatives from the appropriate divisions? IT? Legal? HR? Business line(s)?
- How will you classify the severity of an incident? Have you considered responding to varying degrees and types of incidents?
- Who needs to be notified internally and when? Have you considered when and how management, boards, or customer-facing personnel should be notified?
- When do you need to notify regulators and/or law enforcement? Don't forget to consider recent guidance and proposed legislation and the actions they may require.
- What other third parties need to be involved to contain and control the incident? Have you vetted and retained outside counsel, forensic vendors, e-discovery firms, and/or marketing/PR providers in advance?
- When do you need to notify customers? All 50 states and various federal and industry-specific regulations have their own notification requirements.

There are certainly a host of other considerations that organizations must think through and address in their incident response plans. The time to develop these plans is before an incident occurs. Having a well-developed, current, and comprehensive response plan can make all the difference if and when an actual data incident occurs. As this recent NYDFS action demonstrates, the failure to do so can have serious consequences.

If you have any questions regarding the your cyber risk assessment practices, your incident response planning, testing your incident response plan through tabletop exercises, or any other aspect of your cybersecurity and data protection program, please contact the authors Matt White, CIPP/US, CIPP/E, CIPM or Alex Koskey, CIPP/US, CIPP/E, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.