CLIENT ALERT

Recent Cyber Incidents Likely to Expose Lacking Substance in Risk Assessments and Self-Certifications

Mar.11.2021

Company Hit with $1.5 Million Penalty for Failing to Follow the New York Department of Financial Services Cybersecurity Regulations

In a move that may augur greater enforcement and closer scrutiny of regulated entities, the New York Department of Financial Services (DFS) earlier this month entered into a Consent Order that requires Residential Mortgage Services, Inc. (Residential Mortgage) to pay a civil penalty of $1.5 million for failing to comply with 23 NYCRR 500 (the Cybersecurity Regulation).

The Consent Order states that in early 2019, a Residential Mortgage employee fell victim to a phishing email, and then provided the malicious actor with remote access to her email on four separate occasions through multi-factor authentication approval. The Consent Order states that the employee permitted remote access to her email account even while recognizing that she was not, herself, attempting to access her own email account. After learning about the phishing attack and blocking the remote access, Residential Mortgage took no further action. Moreover, despite taking no further action, Residential Mortgage filed a Certification of Compliance in 2020 attesting that it had complied with the Cybersecurity Regulations throughout 2019.

The failure to act, the Consent Order states, was both "inadequate" and violated the Cybersecurity Regulation that requires covered entities to provide notice to the DFS of "Cybersecurity Events" within 72 hours after they occur. Instead, the DFS only learned of the attack after initiating a safety and soundness examination of Residential Mortgage's cybersecurity infrastructure. The Consent Order notes that Residential Mortgage could have, but failed to, identify whether the employee's email inbox contained private consumer data during the breach, and, if so, could have then determined which consumers were impacted. The failure to comply with the notice requirement also established, the Consent Order notes, that Residential Mortgage's 2020 Certification of Compliance, another requirement of the Cybersecurity Regulation, was inaccurate.

To make matters worse, the Consent Order also states that Residential Mortgage was, at the time of the incident, "missing a comprehensive cybersecurity risk assessment" as required by the Cybersecurity Regulation. The Consent Order explains that a comprehensive cybersecurity risk assessment is supposed to "serve as a means to evaluate cybersecurity risks, and to protect the company's information systems and data, as well as the personal information of its customers" and is supposed to "result in thoughtful cybersecurity programs specifically tailored to safeguard the confidentiality of company and consumer data."

In addition to the civil penalties, Residential Mortgage agreed under the Consent Order to send to DFS for approval a Cybersecurity Incident Response Plan and a Cybersecurity Risk Assessment, and to also send to DFS for approval its plans to monitor for cybersecurity incidents and train its employees. The Consent Order suggests, without saying outright, that the civil penalties were determined in part based on Residential Mortgage's "commendable cooperation throughout the DFS examination and the ensuing investigation."

This is only the second enforcement action that the DFS has brought under the Cybersecurity Regulation, which went into effect in March 2019. The first enforcement was brought against an insurance company in July 2020. As the agency becomes more accustomed (or emboldened) to bring actions against regulated entities, it becomes more important for regulated entities to understand the reporting and compliance requirements. For example, the consequences for failing to maintain adequate cybersecurity risk assessment plans, or for inaccurately certifying that the plan meets the regulatory requirements, may result in substantial penalties – especially if a cybersecurity attack also occurs.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jarno Vanto, CIPP/E, CIPP/US
Partner – New York
Phone: +1 212.803.4025
Email: jvanto@crowell.com

Jacob Canter
Associate – San Francisco
Phone: 415.365.7210
Email: jcanter@crowell.com