NY DFS ENDS THE YEAR WITH MAJOR SETTLEMENTS OVER CYBERSECURITY VIOLATIONS

Britney Lewis

As 2022 was winding down, the New York Department of Financial Services ("DFS") ratcheted up its pursuit of alleged violations of New York's Cybersecurity Regulation ("Cybersecurity Regulation"). Indeed, in the last three months alone, DFS announced two significant settlements. In October 2022, DFS announced a settlement agreement and consent order requiring EyeMed Vision Care LLC ("EyeMed") to pay a $4.5 million penalty to New York for violations of the Cybersecurity Regulation. And in early December 2022, DFS announced that TTEC Health Services LLC ("TTEC") would pay a $1.9 million penalty. These recent settlements should sound the the alarm for DFS-regulated organizations regarding the considerable costs that may be associated with failing to comply with New York's Cybersecurity Regulation.

The EyeMed Settlement

During a weeklong phishing attack that began in June 2020, an outside actor accessed a shared EyeMed email mailbox that was used to process vision care enrollments. The mailbox contained consumer health data—including minors' data—dating back more than six years. Following discovery of the breach, EyeMed notified DFS of the attack and confirmed that the bad actor was able to exfiltrate documents and information while accessing the account.

DFS's investigation into the incident found that EyeMed violated multiple provisions of the Cybersecurity Regulation:

- **Failure to implement multi-factor authentication (MFA).** Although EyeMed (and other covered entities) was required to utilize MFA as of March 1, 2018, EyeMed did not begin implementing MFA until March 2020. The process was not complete until September 18, 2020, and, at the time of the phishing attack, the affected mailbox did not require MFA.
- **Sharing login credentials.** EyeMed also allowed nine employees to share login credentials, including a weak password, to the affected email mailbox. As a result, the compromised mailbox was more vulnerable to cybersecurity threats.
- **Insufficient data disposition processes.** EyeMed failed to implement sufficient data retention and disposal processes in that the affected mailbox contained old non-public information that could (and should) have been disposed of.
- **Failure to conduct adequate risk assessment.** DFS found that EyeMed failed to conduct an adequate risk assessment which could have identified the data disposal risks and risks associated with sharing login credentials for the email

mailbox that was subjected to the phishing attack. DFS explained that EyeMed's engagement of third-party vendors to audit IT controls and Enterprise Risk Management reviews failed to meet the standard for risk assessments.

- **Improper cybersecurity certifications.** As a result of these lack of controls, DFS determined that EyeMed's cybersecurity certifications for the years 2017 – 2020 were improper.

DFS concluded that had EyeMed had adequate controls in place, the phishing attack would have been unsuccessful or at minimum, much more limited in scope. As part of the settlement, EyeMed agreed to undertake significant remedial measures to better secure its data. To begin, EyeMed is required to complete a comprehensive risk assessment within 180 days of the consent order. Following that assessment, EyeMed is required to provide an action plan outlining necessary changes to their cybersecurity controls, written policies, and procedures based on the risk assessment.

The TTEC Settlement

On September 21, 2021, TTEC suffered a ransomware attack where 1,800 devices were compromised. The ransomware attack allowed the perpetrator to exfiltrate non-public information of current and former TTEC employees, as well as current and former insureds of one of TTEC's clients. TTEC quickly reported the ransomware event to DFS in October 2021.

Following its investigation into the TTEC breach, DFS identified three violations of the Cybersecurity Regulation:

- **Failure to implement multi-factor authentication (MFA).** TTEC did not begin to implement MFA until March 2020 (two years after required by the Cybersecurity Regulation) and implementation company-wide was still in progress at the time of the settlement. At the time of the attack, TTEC also had not implemented any reasonably equivalent or more secure access controls.
- **Lack of audit trails.** DFS noted that TTEC did not maintain its audit trail records for three years, as required by the Cybersecurity Regulation, and the audit trail records that it did maintain were insufficient to detect unauthorized access to its systems.
- **Failure to certify or improper cybersecurity certifications.** TTEC failed to file a required certificate of compliance for 2018 and 2019. Additionally, as a result of the other violations DFS identified, TTEC's certification for 2020 was determined to be improper.

In addition to the monetary penalty, TTEC is required to implement remedial measures. First, TTEC must conduct a cyber maturity assessment and submit a report to DFS detailing the findings and steps TTEC will take to address issues identified. Second, TTEC is required to retain a third-party to audit its current MFA controls, as well as its audit trail record retention policy. Finally, TTEC must create an information security dashboard that tracks all information security functions.

Key Implications

These settlements demonstrate that it is critical that covered companies take the time – and now – to ensure their full compliance with the Cybersecurity Regulation. Key action items include:

- **Review Information Governance & Cybersecurity Policies.** Covered entities must ensure that their policies, procedures, and controls align with the Cybersecurity Regulation. Additionally, the recent settlements underscore the importance of periodically conducting risk assessments—both to comply with the Cybersecurity Regulation and to mitigate cyber risks.
- **Embrace Defensible Data Disposition.** Regulators are increasingly focused on reasonable record retention and timely disposition of nonessential personal information. Covered entities should review their record retention and disposal policies and schedules to ensure non-public information is disposed of once there is no longer a legitimate business purpose to retain the information.
- **Cooperate.** Cooperation is key. Both consent orders emphasize that DFS "recognize[d] and credit[ed]" EyeMed and TTEC's "commendable cooperation" during DFS's investigations. Organizations can mitigate the severity of penalties by cooperating with DFS and taking steps to address information security issues.

Looking Ahead

Companies should expect that New York will continue to be at the forefront of enforcing data security laws. In November 2022, DFS released proposed amendments to the Cybersecurity Regulation. The proposed amendments will (i) increase mandatory controls associated with common vulnerabilities; (ii) enhance notification obligations; (iii) require the boards of directors (or other governing individuals) of covered entities to actively monitor cyber risks and approve cybersecurity policies; (iv) limit the numbers of authorized users to modify operating systems and security controls; (v) create a new category of regulated entities for companies that have at least $20 million in annual revenue and more than 2,000 employees or more than $1 billion in annual revenue; and (vi) define each 24-hour period that a violation continues as a separate violation.

Redgrave LLP will continue to monitor the proposed Cybersecurity Regulation amendments and is available to consult and assist in the development and implementation of successful information governance, cybersecurity, and data privacy policies and practices. Establishing good practices for the defensible disposition of nonessential personal information and other non-public information is now essential for many organizations. Even where not mandated by law or regulation, data minimization equals risk mitigation.

For additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.