HINSHAW

New York DFS Fines Mortgage Lender $1.5M for Failure to Report Cyber Breach

Privacy, Cyber & AI Decoded Alert | 2 min read
Mar 11, 2021

The New York State Department of Financial Services (DFS) announced its second enforcement action and first settlement under its cybersecurity regulations (23 NYCRR Part 500). At issue was a licensed mortgage lender's failure to report a "Cybersecurity Event" to DFS within 72 hours of its occurrence and failure to conduct a "comprehensive" cybersecurity risk assessment as mandated by the regulations.

During a routine examination in 2020, DFS examiners discovered that a mortgage lender's employee fell victim to a phishing scam in 2019. The scam allowed a cybercriminal to gain remote access to the employee's email account on four separate occasions before the employee notified the IT department. DFS found the mortgage lender's cyber incident response inadequate. IT staff failed to conduct any further inquiry after discovering the unauthorized access, which DFS called "egregious" given the employee's access to a significant amount of sensitive personal data of mortgage loan applicants, including social security and bank account numbers, obtainable through the email account. DFS cited three specific failures by the mortgage lender:

1. Failure to identify whether the employee's mailbox contained private consumer data during the breach
2. Failure to identify which consumers were impacted
3. Failure to apply applicable state notice requirements triggered by the breach, including notice to DFS within 72 hours

In addition to compliance failures surrounding the breach, examiners found that the mortgage lender was missing a comprehensive cybersecurity risk assessment—despite having filed a certification with DFS that it was in full compliance with the cybersecurity regulations.

In response to the investigation, the mortgage lender retained counsel and a cybersecurity consultant to review all of the employee's emails, identify and make all required notifications to impacted customers and state agencies, and offer credit monitoring and identity theft protection services. DFS noted the mortgage lender's "commendable cooperation" throughout the examination and its commitment to remediation, including having bolstered phishing and other email defenses following the breach. DFS assessed a penalty of $1.5M pursuant to New York Banking Law and required the mortgage lender to submit within 90 days a comprehensive written

incident response plan, risk assessment, and training and monitoring procedures as mandated under the regulations.

Takeaways

DFS examiners are sharply focused on compliance with the cybersecurity regulations. Any company that is not fully in compliance with Part 500 is subject to risk. Notably, there is an emphasis on the contours and functioning of a company's incident response plan, ensuring a full investigation is performed to determine the scope of the breach, the data and individuals impacted. Similarly, employee training on phishing and other employee-targeted scams must be regularly performed, as must testing and monitoring of access and security controls for compliance.

Related Capabilities

Data Privacy, AI & Cybersecurity