BCLP. Client Intelligent

Insights

LESSONS LEARNED FROM NEW YORK'S SECOND CYBERSECURITY ACTION

Mar 31, 2021

SUMMARY

The New York Department of Financial Services (NYDFS) has announced its second regulatory enforcement action against a regulated entity (a New York licensed mortgage banker and loan servicer) for violating NYDFS's Cybersecurity Regulations. The action involved the mortgage banker's failure to report a data breach – a breach caused by an employee overriding the company's multi-factor authentication (MFA) protocol – enabling intruder access. The company agreed to pay a $1.5 million fine and take several actions to bolster its cyber risk and assessment practices.

The unusual data breach, detailed in the Consent Order between the NYDFS and mortgage banker, highlights the need for companies to use more advanced, creative and multi-layered training to prevent their personnel from opening the door to outside intrusions.

The data breach started with a phishing email to an employee who routinely collects large amounts of sensitive personal data from mortgage applicants. The email – which appeared to be from a business partner – directed the employee to a malicious website that asked for a username and password which the employee provided. The data breach still could have been avoided, however, because the company utilized MFA which required the employee to respond affirmatively to an alert on her smartphone. The employee provided the secondary authentication – and did so *four times* that evening after she left work – each time allowing access to her email files. After a fifth attempt the following day, the employee reported the incident.

An internal investigation by the company confirmed the unauthorized access, which it blocked, but that was it. The company did not investigate further, did not ascertain whether customer information had been compromised, and did not report the incident to outside authorities or the NYDFS. Additionally, the breach was not included in the next Certification of Compliance filed by the company's Chief Information Security Officer with the NYDFS. The NYDFS discovered the breach during a routine cybersecurity investigation of the company. The examination also revealed that the

company didn't have a comprehensive cybersecurity risk assessment, which is required by the Cybersecurity Regulations.

This cautionary tale shows the importance of having training practices that are frequent and varied. Breaches cannot be prevented solely through software security, MFA, company protocols and basic personnel training. The company in this instance did have many protocols, such as MFA, and required network access through Active directory with strong, complex passwords. The company utilized both anti-virus and end-point protection software on end-user devices and automated detection rules were in place for transmission of private consumer data, like social security numbers, and the automatic blocking of e-mail redirects by unauthorized actors. Still, none of these protocols were able to prevent this data breach.

Companies will need to be more creative with their training techniques and double down on the frequency of training exercises, adding incentives and disincentives throughout. More advanced training is crucial, as hackers become more sophisticated in the ways they attempt to trick users to override security protocols. Companies may also need to install automatic warning and filtering systems that identify phishing emails before they reach end users and implement IP address filtering systems to block access from suspicious locations. Companies might further consider employing systems that detect anomalies or changes in employees' normal use patterns (e.g., after-hours access) and issue alerts when such anomalies are detected.

As the instant case, however, demonstrates, a well-trained and vigilant work force, at all levels of an organization, will continue to be a crucial line of defense.

For more information about best practices related to the NYDFS Cybersecurity Regulations, see our prior Client Alert.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Insurance
- Consumer Finance Disputes
- Start-Up & Venture Capital Practice
