Reinhart

Is Your Cybersecurity Program Compliant? Lender Penalized $4.25 Million by NYDFS for Deficiencies

Entities operating under the New York Banking Law, Insurance Law or Financial Services Law have another reason to review their cybersecurity programs. In May, the New York Department of Financial Services (NYDFS) published its consent order with OneMain Financial Group, LLC (OneMain), penalizing OneMain $4.25 million for deficiencies in its cybersecurity program under 23 NYCRR Part 500 (the Cybersecurity Regulation).

The Cybersecurity Regulation, promulgated by the NYDFS in March 2017, establishes cybersecurity requirements for banks and trusts, licensed lenders, sales finance companies, insurance companies and any other entities operating under the New York Banking Law, Insurance Law or Financial Services Law (covered entities). The Cybersecurity Regulation requires covered entities to maintain a comprehensive cybersecurity program designed to protect consumer information.

The NYDFS found OneMain's cybersecurity program deficient in a number of ways:

- OneMain's business continuity and disaster recovery (BCDR) plan did not contain necessary information, such as employee contact lists, vendor lists and technical diagrams of systems and networks. Note that the NYDFS is signaling here that simply having a plan is inadequate—the plan must thoroughly address requirements and priorities in the event of a significant disruption.
- OneMain did not appropriately manage user access. It conducted access reviews manually, which introduced human error to thousands of user accounts; its administrative users shared accounts, which were often set to the onboarding default password; and department drives contained files of passwords which, despite being encrypted and password-protected, were also clearly marked "PASSWORDS."
- OneMain did not have an appropriate framework in place to manage development of its in-house applications, resulting in application security issues.
- OneMain did not verify that key cyber personnel maintained current knowledge

POSTED:

Sep 6, 2023

RELATED PRACTICES:

Consumer Finance
https://www.reinhartlaw.com/practices/consumer-finance

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

RELATED PEOPLE:

Kristi J. French
https://www.reinhartlaw.com/people/kristi-french

Jordan Jozwik
https://www.reinhartlaw.com/people/jordan-jozwik

of cyber threats and countermeasures, and it did not track or adequately implement training for its hundreds of information technology personnel.

- OneMain did not follow its own third-party vendor management policy. For example, it allowed vendors to begin working before its due diligence process was complete. Additionally, it did not adjust vendor risk scoring after vendors experienced security events.

These deficiencies generally made OneMain more susceptible to breaches, which it experienced several times between December 2017 and July 2020.

While perfect compliance would not have made OneMain immune to a breach, it may have made breaches less likely and mitigated the harm, and it would have likely minimized the fine assessed by the NYDFS. This consent order serves as a significant reminder for all covered entities to check their cybersecurity programs against the Cybersecurity Regulation and verify compliance.

Current compliance is particularly important given the updated proposed amendments to the Cybersecurity Regulation, published in late June 2023. Once the proposed amendments are in effect, covered entities will have 180 days to comply with even more cybersecurity requirements.

Many of the proposed amendments are related to governance issues. For example, a covered entity's chief information security officer or equivalent would need to be given actual, adequate authority to manage cybersecurity risk, and the entity's board of directors would also need to take an active role in effective oversight, including maintaining a sufficient understanding of cybersecurity matters in order to exercise such oversight.

The proposed amendments would also increase requirements for specific security policies and procedures, requiring multifactor authentication for all remote access to the entity's systems and third-party applications; annual access privilege review; vulnerability monitoring and scanning; controls against malicious code; and annual testing of incident response and BCDR plans, among other things.

The Cybersecurity Regulation already requires covered entities to notify the NYDFS of any cybersecurity incidents within seventy-two (72) hours. The proposed amendments would broaden this to require notification of any extortion or ransom payments made within 24 hours.

Covered entities should review their current cybersecurity programs to verify compliance with the Cybersecurity Regulation. Current compliance will also ultimately aid the transition to comply when the proposed amendments are finalized.

We are monitoring the progress of the proposed amendments to the Cybersecurity Regulation. If you have any questions about the proposed amendments or your current compliance with the Cybersecurity Regulation, please contact Kristi French, Jordan Jozwik or your Reinhart attorney.