BCLP. Client Intelligent

Insights

NYDFS IMPOSES HEAVY FINE AND ADOPTS EXPANSIVE VIEW OF MULTI-FACTOR AUTHENTICATION REQUIREMENTS UNDER CYBERSECURITY REGULATIONS: THE LATEST LESSONS

Apr 26, 2021

SUMMARY

The New York Department of Financial Services (NYDFS) recently announced the resolution, through Consent Order, of its third enforcement action against entities subject to the agency's Cybersecurity Regulations ("Cyber Regulations"). The settlement is notable because it reflects the first public interpretation of the multi-factor authentication (MFA) rule by the NYDFS – an interpretation not evident from the plain text of the rule itself – and the assessment by NYDFS of its largest fine under the Cyber Regulations to date.

In this case, a life insurance and annuities company was ordered to pay a $3 million fine and take other corrective actions because it did not begin to implement MFA for its email system (Microsoft Office 365) and other, unspecified "third-party applications" until more than one year after the MFA rule went into effect (on March 1, 2018). The company also did not complete that process until more than one year later, in August 2020. In the meantime, attackers, using phishing emails, accessed the insurer's internal network on four separate occasions during a two year period from April 2018 through April 2020. The insurer only reported two of the four incidents to NYDFS, but filed a certification attesting to its compliance with the Cyber Regulations for 2018.

The violations came to light during a NYDFS investigation of the two reported incidents. It is not clear why the insurer did not notify NYDFS of the other two incidents because it did report them to other authorities (*e.g.*, the New York Attorney General and FBI). The company also notified the clients whose non-public information had been potentially exposed, changed their account credentials and provided them with credit monitoring. This case thus serves as a reminder to covered entities that they must notify NYDFS of a Cybersecurity Event whenever they are *also required* to notify another "government body, self-regulatory agency or other supervisory body." 23 NYCRR § 500.17(a)(1). Notice to another government agency is not enough.

The Consent Order in this case is especially noteworthy, however, because it reflects the NYDFS's first public interpretation of the regulation governing the circumstances in which MFA is required. Unfortunately, the NYDFS's position seems to raise more questions than it answers.

Section 500.12(b) of the Cyber Regulations requires covered entities to utilize MFA (or a reasonably equivalent tool) for "any individual accessing the Covered Entity's internal networks from an external network." By its terms, Section 500.12(b) thus applies: (1) to any individual, (2) who accesses the internal network, (3) from an external network.

In the Consent Order, however, NYDFS takes the position that Section 500.12(b) also applies to "third-party applications" "that access a Covered Entity's internal network." (Consent Order ¶ 16). There are several issues with this approach.

First, Section 500.12(b) applies to "individuals" who access the internal network, not "third-party applications." The term "third-party applications" is not defined and does not appear anywhere in the Cyber Regulations.

Second, the NYDFS's interpretation appears to ignore language in Section 500.12(b) which requires that access to the internal network originate "from an external network." Apparently, under the agency's view, MFA is required whenever there is access to the entity's internal network regardless of the location from which that access originates. This may be good practice, but that is not what the plain text of the rule provides.

The NYDFS's position could have far-reaching consequences. Under the terms of Section 500.12(b), if an employee were to access a third-party application housed on an external network *from the covered entity's internal network*, MFA would not appear to be required because the individual employee is not accessing the internal network "from an external network." But under the Consent Order, the mere fact that the third party application has access to the entity's internal network suggests that MFA is necessary. Further guidance from the NYDFS would appear to be warranted.

Moreover, as we learned from last month's enforcement action, MFA is not foolproof. In that case, an employee, duped by a phishing email, overrode the company's MFA protocol and gave an intruder access to the entity's internal network on four separate occasions. Plainly, phishing emails and other social engineering scams continue to pose the greatest threat. The Consent Order in the instant case describes MFA as the "first line of defense against attempts to gain unauthorized access." Although that may be true in some respects, we think an entity's most crucial line of defense is a vigilant work force, well-trained at all levels of the organization, to avoid falling victim to phishing emails in the first place.

For more information about best practices for cybersecurity insurers related to the NYDFS Cyber Regulations, see our prior Client Alert.

RELATED PRACTICE AREAS

- Consumer Finance Disputes
- Data Privacy & Security
- Insurance

MEET THE TEAM

Lori Van Auken

New York

lori.vanauken@bclplaw.com
+1 212 541 2053
