NYDFS Updates Cybersecurity Regulation FAQs, Providing Important Clarifications Regarding Exemptions

February 27, 2018

On February 21, 2018, the New York State Department of Financial Services (NYDFS) issued updated Frequently Asked Questions (FAQs) regarding its cybersecurity regulation (Rule), 23 NYCRR Part 500, which establishes stringent cybersecurity requirements for covered entities regulated by the NYDFS. The Rule became effective March 1, 2017, and covered entities were required to certify compliance with the Rule on February 15, 2018.

The original FAQs were published in December 2017, but those FAQs still left questions unanswered. The revised FAQs address some of those questions. Specifically, the NYDFS's revised FAQs address the applicability of the rule to exempt mortgage servicers, not-for-profit mortgage brokers, health maintenance organizations, and continuing care retirement communities.

The revised FAQs provide that exempt mortgage servicers are not covered entities subject to the Rule because the notification that exempt mortgage servicers must provide to the NYDFS is not an "authorization" from the NYDFS. However, exempt mortgage loan servicers that also hold a license, registration, or received approval under the provisions of 23 NYCRR Part 418.2(e) ***are*** still required to prove exemption and comply with the Rule. Additionally, the revised FAQs make clear that the NYDFS "strongly encourages all financial institutions, including exempt Mortgage Servicers, to adopt cybersecurity protections consistent with the safeguards and protections of [the Rule]."

The revised FAQs also clarify that not-for-profit mortgage brokers, health maintenance organizations, and continuing care retirement communities ***are*** covered entities subject to the Rule.

Although the Rule was largely effective in March 2017, the Rule included transitional periods for several key provisions:

- March 1, 2018 – Covered entities are required to comply with sections 500.04(b) (CISO annual report), 500.05 (penetration testing and vulnerability assessments), 500.09 (risk assessment), 500.12 (multifactor authentication) and 500.14(b) (regular training).

- September 3, 2018 – Covered entities are required to comply with sections 500.06 (audit trails), 500.08 (application security), 500.13 (limitation on data retention), 500.14(a) (regular monitoring) and 500.15 (encryption of nonpublic information).
- March 1, 2019 – Covered entities are required to comply with section 500.11 (third-party service provider security policy).

For more information on the Rule, please see our prior alerts on the Rule or contact a member of the firm's Cybersecurity Team.

Related people

Jeffrey Barringer