

New Cybersecurity Requirements Take Effect in New York

April 28, 2017 | [Eric D. Mulligan](#)

New cybersecurity rules from New York's Department of Financial Services went into effect on March 1. The rules apply to any "covered entity," which is any individual or non-governmental entity in a business that requires authorization under the state's Banking Law, Financial Services Law, or Insurance Law. The rules require every covered entity to maintain a cybersecurity program that assesses cybersecurity risks, protects the entity's stored information, and responds to cyberattacks, both successful and unsuccessful, so as to mitigate their harmful effects. Each entity must have a written cybersecurity policy, and a senior officer (or group of senior officers) must approve the policy. Additionally, each entity must designate a "Chief Information Security Officer" responsible for implementing the entity's cybersecurity program and enforcing its cybersecurity policy. The rules also require an entity to conduct regular "penetration testing" of its cybersecurity program, employ qualified cybersecurity personnel, monitor its third party service providers' cybersecurity policies, dispose securely of customer data, encrypt nonpublic information that it holds or transmits, and notify the Superintendent of Financial Services within 72 hours of discovering a cyberattack. There are no specific penalties for violating the rules, but the Superintendent can enforce the rules pursuant to his or her authority under any applicable law.

Massachusetts's Office of Consumer Affairs and Business Regulation has also adopted cybersecurity rules. The Massachusetts rules include an important limitation: they apply only to individuals and entities who own or license personal information of Massachusetts residents. The introduction to the New York rules warns of the risk of "significant financial losses for DFS regulated entities as well as for New York consumers." However, nothing in the New York rules explicitly limits the rules' scope to personal information of New York residents or to individuals and entities who handle such information. Instead, the New York rules apply to any entity subject to the licensing or other authorization requirements of the Banking Law, the Financial Services Law, or the Insurance Law, regardless of whose personal information the entity has. As a result, a covered entity that holds a New York license will be subject to the New York cybersecurity rules, even if it has no personal information of any New York resident. For example, a bank incorporated under New York law will be subject to the cybersecurity rules even if it has no customers in New York.

This result may sound odd in theory, but in practice, it's probably not as strange as it sounds. First, if you went to the trouble of getting the authority to do business in New York, chances are that you serve New York customers and would be subject to the cybersecurity rules even if they applied only to entities that had New Yorkers' personal information. Second, these new rules may be the first cybersecurity rules to go into so much detail about what they require from a business, but they probably won't be the last. Regulators from other states will likely use the New York cybersecurity rules as a model, especially if the rules are effective at preventing or mitigating the harm from cyberattacks on financial institutions.

If you do business in New York and make sure to comply with the state's new cybersecurity rules now, you'll have a head start when other states' regulators strengthen their cybersecurity regulations.

Hudson Cook, LLP, provides articles, webinars and other content on its website from time to time provided both by attorneys with Hudson Cook, LLP, and by other outside authors, for information purposes only. Hudson Cook, LLP, does not warrant the accuracy or completeness of the content, and has no duty to correct or update information contained on its website. The views and opinions contained in the content provided on the Hudson Cook, LLP, website do not constitute the views and opinion of the firm. Such content does not constitute legal advice from such authors or from Hudson Cook, LLP. For legal advice on a matter, one should seek the advice of counsel.

SUBSCRIBE TO INSIGHTS

HUDSON COOK

Celebrating its 25th anniversary in 2022, Hudson Cook, LLP is a national law firm representing the financial services industry in compliance, privacy, litigation, regulatory and enforcement matters.

7037 Ridge Road, Suite 300, Hanover, Maryland 21076
410.684.3200

www.hudsoncook.com

© Hudson Cook, LLP. All rights reserved. Privacy Policy | Legal Notice
Attorney Advertising: Prior Results Do Not Guarantee a Similar Outcome

