

September 14, 2016

NYDFS Proposes Cybersecurity Requirements for Financial Services Companies

By Thomas Dawson and Yuliya Feldman

On September 9, 2016, the New York Department of Financial Services (NYDFS) proposed a long-awaited regulation setting out cybersecurity requirements for financial services companies, including any company authorized to operate pursuant to a “license, registration, charter, certificate, permit, accreditation or similar authorization” under the insurance law.

The proposed regulation appears to be intended to apply very broadly, obviously. Non-U.S. insurers and reinsurers in particular will want to confirm if the proposed regulation applies – whether with respect to excess lines insurers, “trusteed” or “certified” reinsurers. We will report further to clients in this regard.

Background

Since 2013, the NYDFS conducted a series of surveys of its regulated entities regarding their cybersecurity programs, costs and future plans. Beginning in early 2015 the NYDFS began to include cybersecurity assessments when examining insurers and sent so-called “Section 308” letters to domestic insurers requiring extensive disclosure as to insurers’ cybersecurity programs, governance, personnel, practices and procedures. The proposed regulation generally follows the framework set out in prior communications from the NYDFS.

The Proposed Regulation

The requirements set forth in the proposed regulation include the following:

- Establishment of a cybersecurity program, including the adoption of a written cybersecurity policy;
- Establishment of written policies and procedures regarding application security and information systems and nonpublic information accessible to or held by third parties;
- The designation of a Chief Information Security Officer (CISO);
- Employment and training of cybersecurity personnel and training for all personnel;
- Technical requirements, including multi-factor authentication and encryption of nonpublic information;
- Oversight requirements including penetration testing, vulnerability assessments, risk assessments, and audit trail systems;
- Establishment of a written incident response plan and notification to the superintendent in the event of a Cybersecurity Event; and
- Annual certification by senior executives (or possibly by entire Boards of Directors) of compliance, with the first certification due to be filed on January 15, 2018.

The proposed regulation currently specifies an effective date of January 1, 2017 and entities would be given 180 days from that effective date to comply.

Takeaways

The proposed NYDFS cybersecurity regulation presents a more comprehensive framework for cybersecurity than has been seen in any other U.S. jurisdiction. Whether this proposed regulation adequately balances the operational realities of financial services companies with the need to reinforce a) cybersecurity efforts in a world of increasing cybersecurity risks and b) evolving Enterprise Risk Management standards remains to be seen.

It also remains to be seen how this proposed regulation will impact, if at all, other cybersecurity initiatives such as the National Association of Insurance Commissioners' proposed Insurance Data Security Model Law and how New York's "Cybersecurity Event" notification requirements will work with other states' breach notification requirements.

* * * * *

The proposed regulation is subject to a 45-day notice and public comment period before its final issuance. We anticipate that industry organizations and other interested parties will provide the NYDFS with comments. We will review those comments with great interest and will report further as developments warrant.

Insurance Regulatory and Transactional Team

Primary Contacts



Thomas M. Dawson
Partner
New York | London
(212) 248-3160
Thomas.Dawson@dbr.com



Yuliya Feldman
Associate
New York
(212) 248-3172
Yuliya.Feldman@dbr.com

Drinker Biddle®

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | WASHINGTON DC | LONDON

© 2016 Drinker Biddle & Reath LLP. All rights reserved. A Delaware limited liability partnership. Promotional Materials 2016. One Logan Square, Ste. 2000, Philadelphia, PA 19103-6996 (215) 988-2700 office (215) 988-2727 fax
Jonathan I. Epstein and Andrew B. Joseph, Partners in Charge of the Princeton and Florham Park, N.J., offices, respectively.