KING & SPALDING

Client Alert

Insurance Coverage & Recovery Practice Group

February 16, 2018

Do Your Cyber and D&O Policies Cover Emerging Exposures Arising Out Of The New NYDFS Cybersecurity Regulations?

March 1, 2018 will mark one year since the effective date of the New York Department of Financial Services' ("NYDFS") cybersecurity regulations, which may signal a trend towards stricter industry-specific regulatory oversight of companies' cybersecurity practices.[1] The new regulations—which broadly apply to entities subject to New York banking, insurance and financial services laws ("Covered Entities")—impose certain minimum requirements for cybersecurity practices, including, among other things: (i) maintenance of a comprehensive cybersecurity program and corresponding written policies and procedures, including a detailed incident response plan; (ii) designation of a senior officer to implement and oversee the entity's cybersecurity program and policies; (iii) periodic risk assessments and penetration testing; (iv) requirements to notify the NYDFS promptly after discovering a security incident; and (v) annual certification by the board of directors or a senior officer of compliance with the regulations.

Importantly, while the NYDFS regulations provide several transition periods for compliance, Covered Entities must submit their first annual certification of compliance by February 15, 2018, and must complete implementation of other required practices, such as a cyber risk assessment and use of multi-factor authentication, by March 1, 2018.[2] In light of the looming compliance deadlines, companies should assess their directors and officers ("D&O") policies and cyber / data privacy insurance policies now to ensure they provide adequate protection in the event a data breach triggers an expensive NYDFS regulatory investigation or enforcement proceeding.

D&O Insurance – A Potentially Valuable Asset for Boards in the Event the NYDFS Comes Calling After a Data Breach

D&O policies can provide substantial protection to Boards and senior officers for the types of lawsuits and regulatory investigations that can arise out of a data breach. As a general matter, D&O insurance policies cover a company's directors and officers for claims made against them in their individual capacities, as well as "securities claims" made against the company. D&O policies also typically provide coverage to directors and officers who become the target of regulatory investigations or enforcement proceedings, and to companies under certain circumstances (e.g., when a regulatory proceeding is

For more information, contact:

Meghan Magruder
+1 404 572 2615
mmagruder@kslaw.com

Anthony P. Tatum (Tony)
+1 404 572 3519
ttatum@kslaw.com

Shelby S. Guilbert, Jr.
+1 404 572 4697
sguilbert@kslaw.com

Robert D. Griest
+1 404 572 2824
rgriest@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

commenced and maintained against both the company *and* an insured director or officer). Furthermore, most D&O policies in the marketplace today do not contain broad exclusions barring coverage for claims arising out of cybersecurity incidents.

Because the new NYDFS regulations impose new obligations on senior officers, companies should consider whether their D&O policy sufficiently protects individuals who could potentially face exposure to NYDFS investigations or enforcement actions. At a minimum, companies should consider the following issues:

- **Identify New Exposures for Boards and Senior Officers Arising Out of Annual Certification Requirements** – 23 NYCRR 500.17(b) requires a written annual certification of compliance with the new NYDFS cybersecurity regulations, which must be signed by the board of directors or a senior officer(s). The deadline for the first required certification of compliance is February 15, 2018. Because this regulation requires directors and officers to provide a broad certification of compliance covering a twelve (12) month period, which must be supported by documentation, alleged misstatements in these certifications may give rise to regulatory investigations, enforcement actions and follow-on securities claims.
- **Obtain Coverage for the Chief Information Security Officer ("CISO")** – 23 NYCRR 500.04 requires a Covered Entity to designate a CISO to be "responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy." The CISO must also report in writing, at least annually, to the board of directors regarding the company's cybersecurity program. As a result of these new regulatory obligations, Covered Entities should be sure to specifically include their CISO (or equivalent security officer) as an "Insured Person" in their D&O policy.
- **Ensure Regulatory Coverage Includes Coverage for Investigations or Proceedings Brought by the NYDFS and Similar Regulatory Agencies** – 23 NYCRR 500.20 provides that the regulations will be enforced by the NYDFS "under any applicable laws." Covered Entities should carefully review the definitions of key terms like "Claim" and "Loss" in their policies to ensure that claims brought by regulatory agencies, such as enforcement actions, fall within the scope of coverage. While many D&O policies provide coverage for regulatory investigations of Insured Persons, companies should ensure that their D&O policies do not limit the type of governmental agency initiating the matter such that the policy will respond to investigations and proceedings brought by all state and federal authorities. Similarly, and as noted above, both private and public companies should assess the potential availability of coverage for investigations and proceedings brought against the company by the NYDFS.

Possible Implications of the New NYDFS Cybersecurity Regulations for Your Cyber Insurance Program

Procuring rock-solid cyber insurance coverage continues to be challenging due to the evolving cyber risk landscape and wide discrepancies among policy forms currently offered in the market. The new NYDFS regulations will add new complexities to the mix. Companies should carefully review the new regulations and the issues that may arise in the context of cyber insurance, including the following:

- **Avoiding New Potential Pitfalls in the Application and Underwriting Process** – As discussed above, Covered Entities are required to implement a written cybersecurity policy (23 NYCRR 500.03) and incident response plan (23 NYCRR 500.16). Moreover, Covered Entities must annually document any areas, systems or processes that require material improvement, updating or redesign to ensure compliance with NYDFS

cybersecurity regulations, and outline all remedial efforts planned and underway to address such areas, systems or processes (23 NYCRR 500.16). Cyber insurers often ask for detailed information about their policyholders' cybersecurity practices during renewals, and may ask for information about certifications or documentation provided to the NYDFS or other regulators. Moreover, some cyber insurers include regulatory filings and certifications within their policies' definition of the key term "Application," even if they never requested or reviewed those materials when they underwrote the coverage at issue. As exposure to data breach incidents continues to increase, insurers may cite inadvertent errors or omissions in NYDFS certifications as a potential ground for denying coverage after a breach, especially if the certifications formed part of the policy application. To mitigate these concerns, risk managers should pay careful attention to the "Application" definition in their cyber policies, and work closely with their CISO, in-house counsel, and coverage counsel when submitting policy applications to ensure that representations made to insurers concerning cybersecurity practices align with any information that has been (or might be) provided to the NYDFS or other similar regulators.

- **Does Your Policy Require Notification of an Unsuccessful Cyber Attack? –** 23 NYCRR 500.17(a)(2) of the NYDFS regulations requires a Covered Entity to provide notice to the NYDFS within 72 hours of discovering a cyber incident that (i) requires notice be given to any other agency or regulator (e.g., a state attorney general pursuant to a data breach notification statute) or (ii) has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." With respect to the latter requirement, the NYDFS has advised that Covered Entities may be required to report *unsuccessful* cyber attacks that, "in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern." Accordingly, the regulations may require reporting to the NYDFS of a cyber incident that the Covered Entity may not otherwise intend to submit to its insurer for coverage. Companies should review the reporting requirements of their cyber policy to determine whether giving notice to the NYDFS triggers an obligation to notify their insurer, even if the incident itself may not give rise to covered losses under the cyber policy.
- **Ensure Adequate Regulatory Coverage –** As discussed above with respect to D&O insurance, Covered Entities should review their cyber policy to ensure that potential regulatory investigations and enforcement actions are covered third-party "claims." There is now a veritable alphabet soup of regulatory agencies involved in policing companies' cybersecurity practices, and it is impossible to know which ones may respond to a data breach incident. As noted with respect to D&O policies, companies should ensure that the regulatory coverage in their cyber policies is not limited to a short enumerated list of regulators. Also, cyber policies often provide that regulatory coverage is subject to sublimits, meaning that a $10 million cyber policy may only provide $2 million in regulatory coverage. Companies should annually review the sublimits in their cyber policies to ensure adequate cyber coverage for regulatory investigations and proceedings.

In short, the new NYDFS regulations will likely add more uncertainty, and potential liability, to the already-perilous area of corporate cybersecurity. Even companies that do not fall within the NYDFS's jurisdiction should proactively assess how the current trend towards industry-specific cybersecurity regulation may affect them in the near term. Companies should also monitor applicable regulatory guidance that relates to insurance for cyber risks, such as the SEC's 2015 update to investment funds and advisors which counsels such entities to consider whether cyber insurance is "necessary or appropriate."[3] Indeed, the SEC's Division of Corporation Finance has indicated that a company's insurance coverage for cyber risks may be a material component of risk factor disclosures pursuant to Regulation S-K Item 503(c).[4] However, while maintaining a robust insurance program can be an effective tool to mitigate against cyber risks, those risks—and the increasing number of regulations that accompany them—are constantly changing, and

companies must stay aware of new developments to ensure that their policies contain best-in-class terms that adequately protect against their unique risk profile.

We work closely with our clients and their risk managers and brokers to negotiate to navigate the policy renewal process and to improve the wordings of their cyber and D&O policies. We also have assisted our clients recover hundreds of millions of dollars in losses arising from cybersecurity and data breach incidents. Our Cyber Insurance Coverage Recovery practice works closely with our Data, Privacy & Security Practice, which has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of the state and federal government.

---

[1] 23 NYCRR 500, *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[2] For a more detailed discussion of the upcoming NYDFS compliance deadlines, *see* NY DFS Regulation: Certify Your Compliance by February 15 and Assess Your Risk by March 1, King & Spalding Client Alert, February 9, 2018, *available at* https://www.kslaw.com/attachments/000/005/641/original/ca020918b.pdf?1518193873.

[3] SEC Investment Management Guidance Update No. 2015-02, April 2015, *available at* https://www.sec.gov/investment/im-guidance-2015-02.pdf.

[4] SEC Corporation Finance Guidance: Topic No. 2, October 13, 2011, *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.