THOMPSON HINE

Privacy & Cybersecurity Update

November 2022

NY DFS Shakes up Board and Management Exposures for Cyber Breaches

The New York Department of Financial Services ("DFS") published a proposed Second Amendment ("Second Amendment") to Regulation 500 (23 NYCRR 500) on November 9, 2022. The Second Amendment is a proverbial shot across the bow as it directly affects cyber liability for covered entities (financial service entities) regulated by the DFS in the state of New York, including banks, insurers and similar entities. It also significantly impacts liability exposures of the members of boards of directors, "senior officers" (C-suite officers), chief information security officers ("CISO") and possibly some affiliates of covered entities. The Second Amendment was published on November 9th and has a 60-day comment period before it becomes effective. It appears to be on track for adoption with only minor changes.

The Second Amendment raises the compliance bar but also raises questions, including how the proposed new liability provisions will dovetail with the recent protections for C-Suite executives (e.g., CEOs and CFOs) implemented under Delaware's General Corporations Law ("DGCL") that, generally, allow companies to extend limitations for monetary liability and damages for breaches of the generally applied duty of care.

New York

In July and then again in October 2022, the DFS signaled that it would be expanding officers' and directors' exposures for covered entities, at least for cyber-risk responsibilities and corresponding liabilities under New York Regulation No. 500. Those exposures also directly and significantly impact covered entities. In November 2022, the DFS's proposal was formally included in the Second Amendment. In the regulators' view, the Second Amendment largely conforms to the SEC's disclosure requirements under Items 1.05 of Form 8k and 106 (new) and 4.07(j) to Regulation S-K and additional disclosures under Forms 10-Q and 10-K (including 1(c) Cybersecurity to Form 10-K). For a more complete review of these SEC changes, see Thompson Hine's Legal Update, SEC Issues Proposed Rules on Mandatory Cybersecurity Disclosure, dated March 10, 2022.

The most significant proposed changes under the Second Amendment include:

- Increased qualifications, responsibilities and liability of CISOs, "Senior governing bodies" (members of the company's board of directors and relevant committees of the board) and "senior officers."
- The implication that the DFS may be able to reach affiliates of a covered entity if the covered entity relies upon the affiliates for support and even if the covered entity and its affiliates are governed by other governmental authorities and are not doing business in the state. (*See* Section 500.2(d) of the Second Amendment.)
- More explicit requirements for cybersecurity risk audits and assessments and testing, including, in some instances, penetration testing and audits by qualified 3rd parties, particularly for larger or so-called "Class A Companies." (Class A companies have at least $20MM in gross annual revenue during each of the prior two fiscal years (including affiliates in the state) and (1) over 2,000 employees averaged over the last two FY

(including affiliates in or outside of the state) or (2) over $1.0B in revenue in each of that last two FY from all business operations including affiliates. (See proposed amendment.)
- Heightened reporting requirements to regulators including strict timing obligations.
- A reporting provision covering any ransom payments under a ransomware attack.
- Explicit authority of the DFS to impose fines, penalties and sanctions on covered entities that have cyber events. These provisions seem rather draconian given the "people factor" involved in any system and the difficulty in complying with some of the terms of the Regulation and the Second Amendment.

The Second Amendment imposes a heightened level of these obligations on Class A companies only. It also allows limited exemptions for companies that do not qualify as Class A companies, although the exemptions often apply to filings and not to compliance or incident reporting or cyber protection standards. There is a transition period (ranging from 30 days for some sections to 19-months for others) to allow companies to implement the requirements.

The DGCL

Since the mid-80s, the DGCL permitted companies to include charter provisions that limited the personal liability for monetary and certain other damages of the members of the board of directors arising from a director's failure to make an informed decision, resulting in a breach of the duty of care. That liability protection, together with the business judgement rule, in effect, helped directors perform their legal and fiduciary duties without fear of being liable for monetary damages due to a mistake. In August 2022, by statute, those DGCL protections were extended to C-suite officers, (provided, the statutory shield does not extend to claims brought by shareholders on behalf of the corporation against the officers). Overall, assuming the company adopts the DGCL charter provisions, officers and directors will be protected from liabilities arising from allegations of the duty of care, in many instances, including when the director exercises its business judgement, even if there are adverse results for the company. The Delaware standard appears to conflict with the Second Amendment, the latter of which seemingly imposes liability for cyber incident breach on the directors and officers under a lower standard.

Be Prepared

Given the aggressive recent nature of the DFS, this is a clear warning to companies, boards, CISOs and senior executives doing business in or, in some instances, affiliated with covered entities doing business in NYS. Covered entities particularly larger "Class A companies, need to take preparation steps or face the DFS's fines, penalties and other sanctions. (See recent fines and sanctions imposed by the DFS under the Eye Med matter). Companies of all sizes need to prepare now to avoid problems later. Those steps include:

- Ensuring that the company's CISO is qualified and authorized to ensure the company's cyber risks, programs and that information systems are appropriately managed and implemented.
- Board members (including cyber committee members) and senior officers are properly trained and have available resources.
- Internal cyber, data governance and information management policies are up to date and are strictly followed.
- Penetration testing and network security are performed by qualified independent third parties at least annually and monitoring and other assessments implemented and regularly audited, including limiting in-office and remote account access and identity management.
- Employee training is regularly done at least as required and vendor training and agreements are clearly documented and up to date.
- Incident response, disaster and reporting policies, procedures and protocols are in place and all key personnel are fully aware of them, including regulatory reporting requirements are timely met.

Although, *arguendo*, C-suite officers of covered entities may be afforded protections under the DGCL, it is unlikely the DFS will recognize the Delaware statutory and charter protections and allow C-suite officers to wall off cyber related liability exposures under the Second Amendment.

FOR MORE INFORMATION

For more information, please contact:

Robert Ansehl
212.908.3996
Robert.Ansehl@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com