Fisher Broyles

March 2018

Corporate Law Update

Mind Your Bits and Bytes: Cybersecurity Disclosure and Due Diligence

Because the value of today's business is based upon information, it is crucial that companies establish and implement strong policies and procedures to protect their data. The Securities and Exchange Commission recently observed,

> As companies' exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased. Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century.

Accordingly, companies must be sensitive and inform their investors, lenders, and potential purchasers of their approach to information security and any related incidents which have already occurred. Both legal requirements and a desire to 'put your best foot forward' by using a sophisticated approach, make clear the need to do so. Whether a company is disclosing (or, in the case of lenders and acquirers, investigating) information security practices, the following four subtopics should be addressed: (i) security of company trade secrets and other intellectual property in electronic form, and competitive implications; (ii) susceptibility of customer personal information (health and financial) to misuse by identity thieves; (iii) actual security incidents which have occurred; and (iv) susceptibility to operational disruption from wrongful access to materials.

Public Securities Filings.

The need for robust disclosures of cybersecurity risks is most evident in public offerings. While the SEC has been weighing in on the topic since 2011, in late February 2018 the SEC published a detailed statement and interpretive guidance enumerating various matters relating to data security. These issues must be addressed by public companies in 1933 Act filings as well as in periodic and current reports, such as 10-K, 10-Q, and 8-K filings. Cybersecurity should be addressed in the Risk Factor section and the Management Discussion and Analysis discussion, as well as the Legal Proceedings discussion, if

applicable. The SEC's "guidance" should be presumed to have the force of law, at least for those seeking expeditious processing of registrations. Issuers must address both security risks and their implications – e.g. theft of trade secrets such as product formulae or customer lists, or a hack of consumer information – and the nature of their efforts to mitigate such risks, both in technical and operational terms.

The SEC in its recent statement emphasized the importance of adopting strong cybersecurity policies and procedures and of reviewing compliance with such policies and procedures:

> Cybersecurity risk management policies and procedures are key elements of enterprise wide risk management, including as it relates to compliance with the federal securities laws. We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure.

Once the European Union General Data Protection Regulation becomes fully effective after May 25, 2018, the obligations imposed by such EU regulation should be addressed by public issuers in their disclosure filings.

Registered investment companies and advisors are subject to the same and additional standards regarding cybersecurity disclosures, and the SEC's Investment Management division will also scrutinize accordingly.

Private Securities Offerings.

While the SEC has not spoken directly on the matter, prudent issuers in many private offerings should also heed the above admonitions. Among other things, anti-fraud rules are applied in the same manner regardless of whether an offering is public or private. While we expect further guidance to become available regarding what is called for on this topic in each type of private offering, in its absence, issuers should include in their written materials, if any are prepared, the security-related disclosures which are appropriate if the offering were public. Where issuers have contractually committed to ongoing disclosures to investors, this topic should also be taken into account. While, by definition, there will be no SEC comments to deal with in a private offering, failure to address the topic in disclosure documentation may facilitate rescission actions by unhappy investors.

In light of the heightened regulatory scrutiny associated with initial coin offering which we discussed in this space last month, issuers pursuing such transactions should be certain to discuss their cybersecurity risks and practices in appropriate detail in their white papers or other disclosure documents.

Finance.

Outside of the securities context, lenders will seek to mitigate their exposure to borrower business downturns (and worse!) resulting from security incidents by thoroughly addressing the topic in due diligence activity, by having their own pertinent cybersecurity experts to engage with borrower personnel in this area, and by including meaningful warranties and covenants in loan documentation. For example, lenders may wish to require warranties as to (i) absence (or limited scope) of security incidents; (ii) use of 'generally accepted' technical practices such as compliance with Payment Card Industry protocol for credit or debit card transactions (or specific practices, such as encryption, if desired); (iii) management and director oversight of cybersecurity policy and practice; and (iv) effectiveness of third party oversight and formal imprimatur, such as ISO certification. Maintenance of adequate cyber liability insurance may be required in the insurance covenants.

M&A.

Those seeking to engage in M&A transactions should be mindful of the same topics, although in light of various successor liability theories they should be augmented with indemnities for any third-party claims which arise from security breaches. Particular emphasis should be placed on the due diligence phase of the transaction in order for the proposed acquiror to gauge the adequacy of the target's approach to the area and reduce its risk of 'buying a lawsuit,' even one which is indemnified. This due diligence activity should also encompass the target's compliance with the so-called Radio Shack Accord among 30+ state attorneys general governing transfer of consumer information in M&A situations and required privacy policy verbiage. For deals involving large amounts of consumer information, such as credit card numbers or health information, consideration should also be given to extending the survival period for pertinent warranties.

Contacts

If you would like additional information, please contact any of the following FisherBroyles partners:

Atlanta
Carl Johnston
carl.johnston@fisherbroyles.com
(404) 330-8179

Chicago
Marty Robins
martin.robins@fisherbroyles.com
(847) 277-2580

Los Ageles
Steve Papkin
steven.papkin@fisherbroyles.com
(310) 415-6254

About FisherBroyles, LLP

Founded in 2002, FisherBroyles, LLP is the first and world's largest distributed law firm partnership. It has grown to over 240 attorneys in 22 offices nationwide. The FisherBroyles' efficient and cost-effective Law Firm 2.0® model leverages talent and technology instead of unnecessary overhead that does not add value to our clients, all without sacrificing BigLaw quality. Visit our website at www.fisherbroyles.com to learn more about our firm's unique approach and how we can best meet your legal needs.