Cybersecurity Law Report cslawreport.com

Feb. 8, 2023

Financial Services Regulation

Data Breaches and the Private Credit Market: Post-Breach Considerations

By Ryan Blaney, Bharat Moudgil and Evan Palenschat, *Proskauer*

As bad cyber actors become more sophisticated and financial implications of a breach increase, it is critical for stakeholders to consider potential ripple effects on their investment. In the private debt market, it is even more important to consider these impacts given the potentially material costs associated with a data breach, and a primary concern for lenders is that a borrower will expend capital addressing such liabilities that could otherwise be used to service their debt and/or to grow the enterprise. A diversion of funds and increased liabilities on the balance sheet of a borrower could result in financial defaults under a company's credit documents, creating risk of another type.

In this article series, we discuss considerations to prevent and mitigate the effects of a borrower's cyber incident. Part one discussed the cost of breaches, why vigilance is urgent and proactive steps to take to assess a borrower's preparedness. This second part covers how to prepare for and address a borrower's breach.

See "Privacy and Security Due Diligence in M&A Transactions: Going Beyond the Questionnaire" (Jan. 19, 2021).

Preparing for a Borrower's Breach

If a borrower or a guarantor, or any of their subsidiaries or parent entities, has been subject to a cybersecurity incident, lenders should be prepared to address the risks to their capital, and understand what steps to take to protect their investment while considering the dynamic of their relationship with their borrower. Transparency and communication between the borrower and lender are extremely important.

Notification Requirements

First, lenders should check what their existing credit documents require. Credit agreem typically require the borrower to provide notice to the lender upon the occurrence of c ıte- rial events, such as litigation, a labor dispute or a material ERISA liability.

More and more states and federal agencies are requiring accelerated disclosure of cyber incidents. The volume of reports going to states and regulators is expected to increase following last year's guilty verdict against Uber's former security chief officer for not disclosing and concealing a cybersecurity incident. Borrowers should be required to notify the lenders of any data breaches, subject perhaps to a negotiated materiality threshold that is objective (for example, the amount of PII exposure, reasonably expected damages, etc.).

The borrower would then be required to keep lenders abreast of any material or adverse developments going forward, including sources of the breach, potential litigation, associated liability, insurance coverage and steps to remediate the underlying problem and prevent future breaches.

However, unless data security was an issue identified during the legal diligence phase of the transaction, often there is no explicit requirement to notify lenders of a cyber incident that does not rise to the level of a "material adverse effect." Any such requirement negotiated during the documentation phase would be bespoke.

Material Adverse Effect?

In some cases, lenders are required to be notified of an event that would reasonably be expected to have a "material adverse effect." This is a tempting fallback, but ultimately a high bar. Case law on what constitutes a "material adverse effect" is fact specific. Typically, the effects of an event on a business must have been "durationally significant" and be years-long.[1] And in some cases, courts examine whether the parties contemplated such an event when they entered into their agreement and whether either party had any control over the event.

Courts will also focus on the actual impact on the company's business, distinct from any industry-wide shifts. As a result, while a data breach could have a "material adverse effect," the burden will be on the lender to prove that such a breach meets the varied (and in many cases, subjective) requirements of that category.

In the end, it is not common that a lender will be confronted with a cybersecurity incident that is material enough to allow the lender to feel comfortable claiming that the event rises to the level of a "material adverse effect," and even in those situations where it is clear enough, the company will likely be in such financial, reputational or other dire straits that there will be separate breaches of the credit agreement to deal with.

Investor Portals

When there is no specific requirement to notify a lender of a data breach, the lenders may be able to rely on investor portals for making sure they are kept in the loop. For example, public companies need to file an 8-K when an "unscheduled material event" occurs.[2] New Item 1.05 of Form 8-K will require SEC-reporting companies to disclose a material cybersecurity incident within fo[illegible]iness days of determining that a material incident occurred.

See our two-part series on SEC cyber rules: "How to Prepare for the New 8-K Incident Mandate" (Aug. 10, 2022); and "How to Prepare for the New 10-K Disclosure Mandates" (Aug. 17, 2022).

CIRCIA

Private companies may be subject to the Cyber Incident Reporting for Critical Infrastructure Act if they operate in critical infrastructure sectors, which were defined by the Obama Administration to include financial services, telecommunications, information technology, healthcare and energy.[3]

Lenders should be aware of these reporting requirements and could consider making them explicit in the "affirmative covenant" sections of their credit agreements depending on the borrower's industry and vulnerability.

See our two-part series on the new era of cyber incident reporting and cybersecurity regulation: "Key Provisions" (Oct. 12, 2022); and "How Companies Should Prepare and Engage" (Oct. 19, 2022).

Insurance Coverage

Most lenders will want information about the scope of the breach and whether there is dissemination of confidential information, and details regarding the list of affected individuals and types of information disclosed. This, and the circumstances surrounding the breach, will impact whether the associated liability is covered by insurance, or if the expenses will be coming out of the borrower's pocket. If the latter is the case, then lenders should go back to their credit agreements again.

See "Understanding and Evaluating Cyber Insurance in an Evolving Market" (Sep. 2, 2020).

Potential Default

Another source of lender remedies would be available if the underlying data breach has resulted in an event of default under the credit agreement. This would allow the lenders to potentially accelerate the debt (or take other remedies, such as foreclosure on assets) or tighten provisions of the credit documentation in exchange for a waiver of the underlying breach.

The default could occur because of costly and/or adversely decided litigation, or if the company made misrepresentations or acted in bad faith with respect to the risks associated with data breaches.

If a borrower hides a data breach, then failure to notify the lender could also comprise an event of default. Each of these avenues will be subject to qualifiers and thresholds, including "material adverse effect" hurdles, which, as discussed above, could be difficult to cross. However, depending on the underlying facts, these may not be impossible tests for the lenders to meet.

Legal and Regulatory Compliance

Certain representations and warranties are more relevant than others when assessing a breach, such as the general "compliance with laws" requirement. Notwithstanding any materiality qualifiers, there are four "levels" of laws to consider when lenders are negotiating or reviewing the scope of this representation. These four levels are combined in various ways to define the scope of the provision.

1. State Privacy Laws

New state privacy laws have been passed in recent years in places like Colorado[4], Virginia[5], Connecticut[6], and Utah[7], alongside California's landmark CCPA/CPRA[8]. Many other states have proposed privacy legislation in 2023 that may be adopted. There is still no omnibus federal privacy law, but sectoral laws persist in areas such as health and children's data, which could be relevant depending on where a borrower operates.

2. Regulations

Recently, the FTC, SEC and CFTC have become more specific about technical security standards and the handling of personal information. The FTC is also focused on the accuracy of representations that companies are making to customers with respect to their compliance with industry security guidelines or standards.

3. Industry Standards

The most prominent of the industry standards in is the Payment Card Industry (PCI) standard, which is an important standard to meet in the context of vendor and customer contracts.

4. Internal Policies

This adds significant compliance obligations derived from the company's own documentation and agreements with business partners. Complying with one's own privacy policy, privacy notices, or other privacy contractual provisions is essential as state attorneys general and the FTC have deemed failure to do so an unfair and deceptive business practice, even if the privacy policy sets a higher floor than laws or regulations.[9]

Also, the extent of compliance should be scrutinized. Given the likelihood that small infractions will occur with respect to data privacy, materiality and "material adverse effect" qualifiers will commonly be used to limit the representation. Materiality is difficult to assess, however, considering how one click or one oversight could expose the information of millions and cause massive losses.

Lender Liability Issues

When taking actions to address data breaches or cybersecurity weaknesses at its borrowers, lenders should be aware of potential "lender liability" issues. These are rare, but they refer to a theory under which a lender can be held accountable for actions taken (or not taken) by it in connection with a credit facility that results in losses to the borrower or a third party.

Failure to provide financing or, once a loan is active, failing to extend additional capital or forbear from certain actions, could give rise to breach of contract claims. Borrowers could also argue that lender threats or actions in light of a data breach are punitive and have caused duress to the company. And in a situation in which a lender is seen as exerting control over management or interfering with corporate governance, a borrower could call a foul.

To avoid those pitfalls, the aforementioned approaches are at lenders' disposal in the documentation stage. They should conduct fulsome due diligence, and, where possible, tie the risk of data breaches or cybersecurity issues to notice requirements and event-of-default triggers in the credit documents. They could also use cybersecurity improvements as a negotiating trade in exchange for waiving an underlying event of default or their agreement to provide of additional funding.

Remain Vigilant

A U.S. federal omnibus privacy bill was advanced to the U.S. House of Representatives on July 21, 2022. A major point of interest for businesses with consumer data is whether passive consent of a consumer through notice, rather than through affirmative act, is required when collecting the consumer's data.[10] The proposed discussion draft stated in section 2 that consent cannot be inferred by user inaction or the continued use of the product or service. Consent is required in the draft with respect to sensitive categories as well as "aggregated internet search or browsing history." If a similar proposal is advanced in the future, it could have a major impact on internet advertising, and all business dependent on ad revenue.

Regardless of how federal and state privacy and cybersecurity legislation evolves, lenders should remain vigilant. Increases in direct lending to vulnerable industries like health care, financial services, and technology make the need for awareness on this front all the more acute.

See "Takeaways From the New Push for a Federal AI Law" (Oct. 26, 2022).

Ryan P. Blaney is the head of Proskauer's global privacy and cybersecurity group. He is based in Washington, D.C.

Bharat Moudgil is a partner in the firm's private credit group and is based in Los Angeles.

Evan Palenschat is a partner in the firm's private credit group and is based in Chicago.

[1] S. Montgomery, B. Moudgil and S. Lam, Exceptions in credit agreements addressing Covid-19 crisis, Los Angeles & San Francisco Daily Journal, May 6, 2020.

[2] *See*, Form 8-k, Item 8.01. 17 CFR 249.308.

[3] *See Cyber Incident Reporting for Critical Infrastructure Act of 2022*, *H.R. 2471, 116th Cong. (2022).*

[4] *See generally*, Colorado Privacy Act, Senate Bill 21-190, 73d Leg., 2021 Regular Sess. (Colo. 2021), to be codified in Colo. Rev. Stat. ("C.R.S.") Title 6.

[5] *See generally*, Va. Code Ann. § 59.1-576.

[6] *See generally*, Connecticut P.A. 22-15.

[7] *See generally*, UCPA § 13-61-102(1).

[8] *See generally*, Cal. Civ. Code § 1798.140.

[9] "In many [privacy and security] cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce." *Privacy and Security Enforcement*, Federal Trade Commission.

[10] *See* H.R.8152 - American Data Privacy and Protection Act, Sec. 102, 202, 204.