SEC Enforcement Action Against Blackbaud, Inc. Highlights Scrutiny of Issuer Disclosures after Ransomware Attack

March 23, 2023 Tim Newman, Kurt Gottschall

PRACTICES Corporate, Privacy and Cybersecurity

In the wake of ransomware attacks or other cybersecurity breaches, issuers are naturally focused on containing operational and reputational damage, and securing their systems going forward. However, this client alert illuminates another critical task: ensuring that public disclosures remain accurate as investigations regarding cyber events unfold.

In a cautionary tale, data management company Blackbaud, Inc. recently agreed to pay a $3 million penalty to settle SEC charges stemming from the company's alleged disclosure failures following a 2020 ransomware attack. According to the order, Blackbaud allegedly made materially misleading statements in its securities filings during a short, two-month time frame regarding the ransomware attack and allegedly failed to maintain adequate disclosure controls designed to ensure that required information was accurately and timely disclosed to investors.

Background

On May 14, 2020, Blackbaud, a company that provides data management software to nonprofit organizations, detected unauthorized access to the company's systems. Blackbaud cybersecurity personnel, along with third-party vendors, conducted a preliminary investigation and ultimately paid the ransom in exchange for the attacker's promise to delete any exfiltrated data.

On July 16, 2020, Blackbaud disclosed the incident on its website and notified impacted customers. The disclosure stated that "[t]he cybercriminal did not access … bank account information, or social security numbers." By the end of July, however, Blackbaud's cybersecurity personnel learned that the attacker had in fact accessed bank account information and social security numbers in unencrypted form. According to the SEC, senior management at Blackbaud responsible for investor disclosures were not told the full nature of the breach, and the company allegedly did not have procedures in place to ensure that such information was communicated to management and ultimately to investors.

On August 4, 2020, the company filed a Form 10-Q in which it allegedly failed to disclose the unauthorized access of bank account information and social security numbers, stating only that "the cybercriminal removed a copy of a subset of data." The Form 10-Q also stated, "A compromise of our data security that results in ***customer or donor personal*** or payment card data being obtained by unauthorized persons ***could*** adversely affect our reputation … as well as our operations …." The SEC took issue with this disclosure, finding that it "misleadingly characterized the risk of exfiltration of such sensitive donor information as hypothetical."

Approximately two months later, Blackbaud filed a Form 8-K on September 29, 2020 containing details of the incident. The company noted for the first time that the ransomware attack may have resulted in access to customer bank account information and social security numbers. Blackbaud

simultaneously began notifying clients for whom such sensitive donor information had been exfiltrated.

In its order, the SEC found that Blackbaud had failed to maintain appropriate disclosure controls and procedures. The SEC also found that Blackbaud had violated the non-scienter anti-fraud provisions of the Securities Act in light of Blackbaud's offer and sale of stock to employees through an equity and incentive compensation plan in effect during the relevant time period.

To settle the matter, Blackbaud agreed to pay a $3 million civil penalty and to cease and desist from committing or causing any future violations.

SEC's Increased Focus on Cybersecurity

Last year, SEC Chair Gary Gensler reiterated that the SEC would continue to prioritize cyber enforcement, and the agency nearly doubled the Enforcement Division's Crypto Assets and Cyber Unit. The recent charges against Blackbaud highlight the agency's increased activity related to cybersecurity incidents and disclosures.

The SEC has also proposed a comprehensive rule to standardize and enhance disclosures relating to cybersecurity risk management, strategy, governance, and incident reporting by public companies. Among the other things, the proposed rule would require public companies to report in a Form 8-K any material cyber incidents within four days of concluding that an incident was material. Public companies would also be required to provide updates on the incidents in Forms 10-K and 10-Q. The proposed rule would also amend Regulation S-K to require companies to describe their policies and procedures for identifying and managing risks from cyber threats and to make certain disclosures regarding cybersecurity governance. Such disclosures would include board oversight of cybersecurity risk, how the board is informed about those risks, and management's role in implementing cybersecurity policies and procedures.

These proposals are expected to be finalized and adopted soon.

Key Takeaways

- The order against Blackbaud underscores an issuer's obligation to make timely and accurate disclosures relating to cybersecurity incidents. To do so, issuers should ensure that their disclosure controls are designed to promptly escalate material information regarding the extent of cyber breaches as investigations evolve. Issuers should be particularly cautious in attempting to describe the extent of sensitive data compromised (e.g. bank accounts and social security numbers) in cyber attacks while relevant investigations remain ongoing.
- Issuers should also regularly assess recurring or boilerplate cybersecurity risk disclosures to confirm they remain materially accurate following cybersecurity incidents or breaches. The Blackbaud case provides yet another example that the SEC often alleges issuer disclosures of "hypothetical" risks or facts are misleading when those facts have already transpired.
- Finally, issuers should monitor the SEC's anticipated cybersecurity rule changes for public companies. When those rules become effective, issuers should reassess their cybersecurity policies for compliance with those changes. Issuers also should expect that the SEC will carefully review the accuracy and consistency of cybersecurity incident updates in Forms 10-Q and 10-K.

For more information about the SEC's settlement with Blackbaud, the SEC's anticipated cybersecurity disclosure rules, and other topics related to the SEC's focus on cybersecurity, contact

one of the Haynes Boone lawyers below.