Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

JUNE 15, 2020

Board Directors Beware: Potential Liability in Data Breach Suit

Events Giving Rise to the Complaint against LabCorp Directors and Officers

On April 28, 2020, a shareholder of Laboratory Corporation of America Holdings, more commonly known as "LabCorp," commenced a derivative action against LabCorp, and several of its individual directors and officers. The complaint arises out of two major data security incidents and principally alleges that the individual defendants breached their fiduciary duties in a myriad of ways.

LabCorp is one of the leading providers of diagnostic medical testing services in the world and offers a variety of clinical testing services. Testing more than 2.5 million patient specimens on a weekly basis, the lab giant processes a staggering amount of personally identifiable information (PII) and personal health information (PHI). In offering its services to patients, LabCorp generates invoices to bill patients, which are then forwarded to a collection agency, such as American Medical Collection Agency (AMCA), if they are not timely paid.

It is LabCorp's relationship with AMCA that led to the first data breach giving rise to this lawsuit. Analysis from a cybersecurity firm revealed that a large number of compromised payment cards and associated PII from AMCA were on the dark web. The security audit revealed that the information was likely stolen from AMCA's payment portal during a nearly eight-month breach. The complaint alleges that this breach "directly impacted and affected millions of LabCorp patients."

On May 14, 2019, LabCorp was notified of the breach, and it informed investors of the same on June 4, 2019 through an SEC filing. The delay in notifying investors is one of the ways the defendant directors and officers are alleged to have breached their fiduciary duties. The company's June 4 public disclosure of the data breach (less than one month from receiving notice of the breach) drew national attention and prompted a series of inquiries from U.S. senators, state attorneys general and various other state and federal agencies. In addition to this derivative action, a class action brought by patients whose information was compromised as a result of the first breach is also pending in the District Court of New Jersey.

LabCorp allegedly suffered a second data breach in January 2020 when "an unprotected web address granted access to LabCorp documentation containing PHI." The complaint states that LabCorp was informed of this breach on January 28, 2020. However, neither the company nor the individual defendants have publicly addressed the second breach or acknowledged that it in fact occurred.

This shareholder derivative action was brought in response to both data breaches.

Specific Allegations in Complaint

The fundamental claim made in the complaint is that LabCorp had insufficient cybersecurity practices and inadequate oversight of AMCA. Most of the claims relate to the allegation that the individual defendants, directors and officers of LabCorp, breached their fiduciary duties of care, loyalty and good faith. The complaint specifically alleges that these duties were breached when the individual defendants:

- failed to implement effective systems to protect patient PII and PHI;
- failed to exercise appropriate oversight by not monitoring LabCorp's compliance with state and federal regulations;
- provided PII and PHI to a LabCorp business associate with deficient cybersecurity and breach detection;

- failed to ensure that LabCorp and its business associates used proper cybersecurity safeguards to adequately protect patient PII and PHI;
- failed to timely notify potentially affected individuals;
- failed to make adequate public disclosures following the data breaches;
- allowed LabCorp to violate unspecified state and federal laws; and
- failed to review and affirm or revise LabCorp's existing data security policies and procedures.

Each of these alleged failures is characterized as evidence that the shareholders intend to prove through the litigation and trial, that LabCorp's directors and officers did not act, and continue to not act in the best interest of the company.

Key Takeaways

Though the litigation is in its early stages and dispositive motions have yet to be made, the allegations raise several important points that businesses would be wise to keep in mind.

- Companies should regularly review their data privacy and cybersecurity policies and revise accordingly. As the legal landscape of cybersecurity is constantly evolving, regular review of internal practices will help prevent internal controls from becoming stale.
- Employees charged with handling and processing PII and PHI should be properly trained in how to do so in a safe and secure manner. This is an obligation imposed by several laws such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the New York SHIELD Act, and simply is a best practice even in the absence of a legislative mandate. Employees should also be sufficiently well-versed in the data privacy and cybersecurity laws that apply to their employer's business.
- Third-party risk and management are critical. The vendors and third parties to which a company discloses PII and/or PHI should be appropriately vetted at the onboarding stage and regularly evaluated and monitored depending on the level of risk associated with the type of data such vendor receives and manages for the company. A third party's data privacy and cybersecurity practice should be assessed for competence prior to disclosing PII and/or PHI. Organizations should impose contractual requirements on third parties even in the absence of a statutory or regulatory obligation to do so.
- Security audits are a critical tool for understanding potential vulnerabilities in an organization's (and it's third-party vendors') data privacy and cybersecurity programs.
- The long-term cost of inadequate data privacy and cybersecurity practices can be exorbitant. For instance, LabCorp spent an estimated $11.5 million in out of pocket costs on response and remediation costs following the first data breach. Remarkably, this figure does not include any litigation-related expenses associated with defending this action or the patients' class action. Giving compliance efforts due attention in advance may be well worth the effort in light of the high cost of rectifying a data breach after the fact.

For more information about data privacy and cybersecurity best practices and compliance, please contact Jessica Copeland, Hannah Redmond or any of the attorneys in the Cybersecurity and Data Privacy practice.

BOND SCHOENECK & KING ATTORNEYS