SAUL EWING ARNSTEIN & LEHR LLP

ALERT

Cybersecurity and Privacy Practice

Higher Education Practice

SEPTEMBER 2020

Higher Education Institutions and Nonprofit Organizations Face Potential Wave of Lawsuits Over Blackbaud Data Breach

Alexander (Sandy) R. Bilus

On September 21, 2020, a putative class action lawsuit was filed against the President and Fellows of Harvard College, Bank Street College of Education, and the Lower East Side Tenement Museum in connection with an alleged data breach. *See Cohen v. Blackbaud, Inc. et al.,* No 2:20-cv-01388 (W.D. Wash.). The suit also names each defendant's software and service provider Blackbaud, Inc., whose systems were breached last spring in an apparent ransomware attack. Many higher education institutions and nonprofit organizations use Blackbaud platforms to manage fundraising activities and store personal information, and thus have been impacted by this attack. The plaintiff claims that the breach was the result of the defendants' unreasonable and deficient data security practices, and seeks to bring claims on behalf of a nationwide class of individuals whose information was accessed in the data breach. A number of other similar lawsuits have already been filed against Blackbaud over this incident, but the *Cohen* lawsuit appears to be the first one that names Blackbaud's customers—including higher education institutions—as defendants. Given the widespread use of Blackbaud's services by higher education institutions and other nonprofit organizations, this lawsuit could be a forerunner to future lawsuits brought against other institutions that entrusted Blackbaud with the personal information of their students, alumni and donors. This alert discusses the data breach, the plaintiff's claims, and some potential defenses that institutions should consider if they are named as defendants in similar lawsuits.

The Blackbaud Breach

Blackbaud has publicly disclosed certain details about the incident that is at the heart of the *Cohen* lawsuit. According to Blackbaud, in May the company discovered that it had been the target of a ransomware attack in which a criminal attempted to disrupt the company by locking it out of its own data and servers. Blackbaud says that it was able to stop the attack and expel the intruder from its system, but the attacker was able to transmit a copy of a subset of data outside of Blackbaud's system. Blackbaud paid the attacker's ransom demand and received confirmation from the attacker that the copy of the data had been destroyed. Blackbaud claims that "[b]ased on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly."

The Allegations in the *Cohen* Lawsuit

Despite Blackbaud's statement that the stolen data had been destroyed and that it will not be misused, a number of class action lawsuits have already been filed against Blackbaud over the alleged harm that the incident caused to individuals whose data the criminal accessed. *See, e.g., Arthur et al. v. Blackbaud, Inc.,* No. 2:20-cv-14319 (S.D. Fl.); *Allen v. Blackbaud, Inc.,* No. 2:20-cv-02390 (D. S.C.); *Eisen v. Blackbaud, Inc.,* No. 2:20-cv-08356 (C.D. Cal.). But the *Cohen* lawsuit appears to be the first instance of a plaintiff naming Blackbaud's customers as defendants in addition to Blackbaud itself.

In the *Cohen* lawsuit, the plaintiff claims that the Blackbaud breach occurred sometime between February and May 2020, but that Blackbaud did not notify its customers until July 2020. In turn, after being notified by Blackbaud in July, the defendants (including Harvard) allegedly "unreasonably and wrongfully delayed in providing notification and did not even begin to inform those affected until around August 2020." The plaintiff alleges that the defendants failed to "properly monitor the computer network and systems that housed the Private Information; failed to implement appropriate policies; and failed to properly train employees regarding cyberattacks." The plaintiff further alleges that "[h]ad Defendants properly monitored their networks, security, and communications, they would have prevented the Data Breach or would have discovered it sooner."

The plaintiff brings multiple claims on behalf of the putative class, including negligence, breach of contract, violation of state consumer protection acts, and violation of state data breach acts. The plaintiff claims that he and the other class members have suffered damages because their stolen information may have already been misused, they are now exposed to a heightened risk that their information will be misused in the future, they have incurred a loss of value in their information, they purchased identity theft protection in an attempt to minimize the risks to their information, and they are still incurring ongoing damages while waiting for the defendants to complete their investigation of the incident.

The plaintiff seeks damages, including punitive damages, and an injunction requiring the defendants to maintain reasonable security measures.

Potential Defenses to the Lawsuits

Blackbaud provides services to many higher education institutions and other nonprofit organizations, and it is likely that other "copycat" lawsuits will soon be filed against other institutions over the Blackbaud breach. Accordingly, organizations that are facing this risk should begin evaluating their potential defenses to such a lawsuit. The list below is not exhaustive and focuses primarily on arguments that can be raised at the motion to dismiss stage of a lawsuit, but organizations should consider the following:

- ***Lack of standing.*** Courts in some jurisdictions have dismissed data breach class actions for lack of standing, concluding that the plaintiffs are unable to demonstrate that they have suffered an "injury in fact." Courts have reasoned that data breach victims are only alleging hypothetical, possible future injuries that could result from a breach rather than concrete, actual harm. Thus, these courts have concluded, there is no "case or controversy" and no standing under Article III of the United States Constitution. Note, however, that courts are split on this issue, and some jurisdictions have rejected this reasoning.

- ***Failure to adequately allege damages.*** Other courts have concluded that, although data breach victims may have standing, they have failed to adequately allege all of the elements of their claims, and have dismissed cases on this basis. In particular, courts have concluded that plaintiffs have failed to allege the damages element of their claims. Like the plaintiff in the *Cohen* lawsuit, plaintiffs have claimed that their damages have included potential future misuse of their information as well as diminution in the value of their information, and some courts have concluded that these allegations are too tenuous to constitute damages as an element of a cause of action.

- ***Lack of personal jurisdiction.*** The *Cohen* lawsuit was filed in Washington even though none of the defendants are located in that state. Accordingly, the defendants might be able to raise a personal jurisdiction defense against the lawsuit. To the extent future lawsuits are also filed across the country against other institutions, those institutions may be able to present the same defense.

- ***Failure to state a claim under state data breach laws.*** Another possible argument to raise at the motion to dismiss stage is that state data breach notification laws do not create a private cause of action. Instead, state government officials – typically the state attorney general's office – are responsible for enforcing violations of these laws. Thus, courts should dismiss such claims when brought by private plaintiffs alleging that a defendant failed to adequately protect data or timely notify individuals of a breach of that data.

- ***Failure to state a claim under state consumer protection laws.*** To the extent a plaintiff brings a claim under a state consumer protection law, a defendant might be able to argue that it had not made any particular promises to the plaintiff about the adequacy of its data security policies and practices, and thus that it had not made any affirmative misrepresentation. But even if a defendant has said nothing in the past about its data security, a plaintiff might argue that a defendant's failure to disclose that it did not provide adequate security was itself enough to state a claim for a violation of the law.

- ***Failure to trace any harm to this particular incident.*** To the extent a plaintiff is able to show that his or her personal information has actually been misused, an institution might be able to point to other breaches of other organizations or businesses that exposed the same person's information. Given the prevalence of data breaches, it is becoming increasingly likely that the same personal information has been released multiple times, making it difficult for a plaintiff to trace any harm to one particular incident.

- ***Defenses against class certification.*** The "multiple breach" issue discussed above also could present problems for certifying a class, since different members of the class will have been affected by different breaches. A defendant could argue that because of this multiple breach issue, any questions of law or fact common to the class members do not predominate over questions affecting only individual members, or that the claims or defenses of the representative plaintiff are not typical of the claims or defenses of the class. Other commonality/typicality-type arguments against class certification might assert that class members will have varying types of personal information impacted, did not respond in a uniform manner to the breach, and been provided different privacy notices and statements relating to data security.

The legal landscape for data breach cases is still developing, of course, and the viability of any of these arguments will depend on the facts alleged in any particular case and the law in that jurisdiction.

Saul Ewing Arnstein & Lehr LLP attorneys are actively monitoring the *Cohen* lawsuit and the other Blackbaud ransomware class actions, as well as other data security issues affecting higher education institutions. If you have questions about this alert, please contact the author.

This alert was written by Alexander R. Bilus, vice-chair of the Firm's Cybersecurity and Privacy Practice and a member of the Firm's Higher Education Practice. Alexander can be reached at (215) 972-7177 or at Alexander.Bilus@saul.com. This alert has been prepared for information purposes only.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.