Tucker Ellis LLP

Are You Affected by the Blackbaud Ransomware Attack?

AUGUST 2020

In July, Blackbaud, a U.S.-based cloud computing provider and one of the world's largest providers of education administration, fundraising, and financial management software, notified users of its services that it had suffered a ransomware attack in May 2020 in relation to personal data stored on its servers. Numerous colleges, universities, high schools, foundations, and other nonprofits across the U.K., U.S., and Canada were affected. While unsuccessful in blocking access to the database targeted in the attack, the cybercriminal was able to remove a copy of a subset of several of Blackbaud's clients' data. Blackbaud has indicated that the compromise persisted over three months, from February 7 to May 20, 2020.

Blackbaud faces criticism for taking many weeks to inform its customers of the breach. Additionally, Blackbaud's handling of the attack has raised some questions. The company's notice to its customers asserts that it paid the cybercriminal's ransom and that it somehow confirmed that the cybercriminal's copy was destroyed and not further shared. While paying ransom demands is not unlawful, it goes against the official advice issued by many law enforcement agencies, including the FBI.

Whether or not your organization's data was compromised in the Blackbaud attack, the incident serves as an excellent reminder of what to do in the event your data is compromised one way or another. In addition to reviewing Blackbaud's notice and suggested resources, organizations should consider the following steps, which apply generally, regardless of the scope and nature of a cyberattack:

1. **Consult your incident response plan, customer notification policies, vendor contracts, and cyber insurance coverage.** Some data breach insurance coverage comes with incident response resources, including payment for breach counsel and forensic IT firms.
2. **Know exactly what categories of personal information were likely compromised.** If personal or financial account information was not accessed and was properly encrypted, most data breach notification laws will not be triggered; however, the legal definition of protected personal information varies by statute, by state, and by country.
3. **Know where potentially impacted constituents are located.** Breach notification requirements vary by jurisdiction. Individuals located in the European Union, for

example, have broader rights regarding their personal information, which may require notification not required elsewhere. Prompt reporting and consultation may also be required by the applicable EU member state data protection authority under the GDPR.

4. **Document your incident response and decision making.** Whether you decide to notify constituents or not, document your investigation, analysis, and decisions. In most cases, it is the data "owner" and not the service provider who is accountable for ensuring the protection of personal information. If ever called upon to demonstrate that you took appropriate action, your documentation should serve you well.
5. **Tucker Ellis is here for you.** No matter the nature and extent of the data breach you are facing, Tucker Ellis is here to guide you through the legal questions you may have concerning your notification obligations, potential liability, and how to mitigate the risk of future attacks.

If you have any questions or would like additional information, please contact any member of our Privacy & Data Security Group.