Blackbaud Settles Multistate Data Breach Investigation for Nearly $50 Million

On Oct. 5, 2023, software vendor, Blackbaud, entered into a $49.5 million settlement with 49 state attorneys general and the District of Columbia. The settlement resulted from a finding that Blackbaud's cybersecurity and privacy procedures proved inadequate in response to its 2020 ransomware attack that led to millions of consumers' personal information being compromised.

Blackbaud provides software services to nonprofit organizations, such as charities, educational institutions, healthcare institutions, and religious and cultural organizations. As part of its business, Blackbaud manages data about their consumers, including social security numbers, protected health information and contact and demographic information.

A multistate investigation led by the attorneys general in Indiana and Vermont found that Blackbaud violated state consumer protection laws, breach notification laws and the Health Insurance Portability and Accountability Act (HIPAA). Specifically, Blackbaud learned of the breach on May 14, 2020, but did not publicly disclose the data breach until July 16, 2020. Blackbaud also failed to notify its affected consumers promptly, completely or accurately. Furthermore, being a business associate to several customers that are HIPAA covered entities, Blackbaud failed to have appropriate administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of any protected health information.

In addition to the monetary penalty, Blackbaud must strengthen its security and breach notification practices. Specifically, Blackbaud is required to implement incident and breach response plans; personal and protected health information safeguards and controls; employee training resources; specific technical safeguards and controls, such as network segmentation and risk assessments; and a comprehensive information security program. Blackbaud is also prohibited from making misleading statements regarding its data protection, privacy, security, confidentiality, integrity and breach notification requirements. Lastly, for seven years Blackbaud must obtain third-party assessments of its compliance with the settlement.

Multistate data breach investigations have been on the rise in recent years. This settlement emphasizes the importance of having robust and up-to-date cybersecurity and privacy practices. This multistate sanction of Blackbaud should also serve as a reminder for organizations to have advanced incident response plans that foster expedient response and notification practices.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including HIPAA and other privacy authorities. If you have any questions about the information presented in this memo, please contact Jessica Copeland or any attorney in Bond's cybersecurity and data privacy practice.

**Special thanks to Associate Trainee Victoria Okraszewski for her assistance in the preparation of this blast. Victoria is not yet admitted to practice law.*

BOND SCHOENECK & KING ATTORNEYS