PRESS RELEASE | October 6, 2023

AG Fitch Announces $49.5 Million Multistate Settlement with Blackbaud for Data Breach Impacting Millions of Consumers



When a breach has occurred, we expect companies to notify affected people in a timely and complete manner to prevent further exposure and damage. I am pleased that Blackbaud has agreed to strengthen its data security and breach notification process, and it is my hope that this serves as a notice that those who fail to protect users' personal information will be held accountable.

Lynn Fitch

(Jackson, Mississippi) Attorney General Lynn Fitch announced today that Mississippi, along with 49 other states, reached a settlement with software company Blackbaud regarding a 2020 ransomware event that exposed the personal information of millions of consumers across the United States. Under the settlement, Blackbaud has agreed to overhaul its data security and breach notification practices and make a $49.5 million payment to states. Mississippi will receive $547,684.

"With nearly every aspect of our lives managed online, it is essential for the gatekeepers to exercise vigilance with individuals' sensitive personal information," **said General Fitch.** "When a breach has occurred, we expect companies to notify affected people in a timely and complete manner to prevent further exposure and damage. I am pleased that Blackbaud has agreed to strengthen its data security and breach notification process, and it is my hope that this serves as a notice that those who fail to protect users' personal information will be held accountable."

Blackbaud provides software to various nonprofit organizations, including charities, higher education institutions, K-12 schools, healthcare organizations, religious organizations, and cultural organizations. Blackbaud's customers use Blackbaud's software to connect with donors and manage data about their constituents, including contact and demographic information, Social Security numbers, driver's license numbers, financial information, employment and wealth information, donation history, and protected health information. This type of highly sensitive information was exposed during the 2020 data breach, which impacted over 13,000 Blackbaud customers and their respective consumer clients.

Today's settlement resolves allegations by the attorneys general that Blackbaud violated state consumer protection laws, breach notification laws, and HIPAA by failing to implement reasonable data security and remediate known security gaps, which allowed unauthorized persons to gain access to Blackbaud's

network, and then failing to provide its customers with timely, complete, or accurate information regarding the breach, as required by law. As a result of Blackbaud's actions, notification to the consumers whose personal information was exposed was significantly delayed or never occurred.

Under the settlement, Blackbaud has agreed to strengthen its data security and breach notification practices going forward, including:

- Prohibition against misrepresentations related to the processing, storing, and safeguarding of personal information; the likelihood that personal information affected by a security incident may be subject to further disclosure or misuse; and breach notification requirements under state law and HIPAA.
- Implementation and maintenance of incident and breach response plans to prepare for and more appropriately respond to future security incidents and breaches.
- Breach notification provisions that require Blackbaud to provide appropriate assistance to its customers and support customers' compliance with applicable notification requirements in the event of a breach.
- Security incident reporting to the CEO and Board, enhanced employee training, and appropriate resources and support for cybersecurity.
- Personal information safeguards and controls requiring total database encryption and dark web monitoring.
- Specific security requirements with respect to network segmentation, patch management, intrusion detection, firewalls, access controls, logging and monitoring, and penetration testing.
- Third-party assessments of Blackbaud's compliance with the settlement for 7 years.

Indiana and Vermont co-led the multistate investigation, assisted by Alabama, Arizona, Florida, Illinois, and New York, and joined by Alaska, Arkansas, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Hawaii, Idaho, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

###

Media Contact
Debbee Hancock
Debbee.Hancock@ago.ms.gov