The Office of the Attorney General (https://portal.ct.gov/ag)
William Tong

Attorney General Tong Announces $49.5 Million Multistate Settlement with Blackbaud for Data Breach Impacting Thousands of Nonprofits and Millions of Consumers

Press Releases

OFFICE OF THE ATTORNEY GENERAL
CONNECTICUT
LEX ET JUSTITIA

10/05/2023

Attorney General Tong Announces $49.5 Million Multistate Settlement with Blackbaud for Data Breach Impacting Thousands of Nonprofits and Millions of Consumers

(Hartford, CT) -- Attorney General William Tong joined 49 other attorneys general today announcing a settlement with software company Blackbaud for its deficient data security practices and response to 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. Connecticut will receive $602,303 from the settlement.

"Blackbaud collected highly sensitive consumer data, including Social Security numbers, protected health information and financial records. They had an obligation to safeguard this information, and they failed. Our settlement forces Blackbaud to adopt stringent data security and breach notification practices going forward. In coordination with attorneys general nationwide, we will aggressively enforce our data security laws," **said Attorney General Tong.**

Blackbaud provides software to various nonprofit organizations, including charities, higher education institutions, K-12 schools, healthcare organizations, religious organizations, 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 constituents.

Today's settlement resolves allegations of 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 at all insofar as Blackbaud downplayed the incident and led its customers to believe that notification was not required.

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 the Executive Committee consisting of 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.

Assistant Attorney General Kileigh Nassau and Deputy Associate Attorney General Michele Lucan, Chief of the Privacy Section assisted the Attorney General in this matter.

Twitter: **@AGWilliamTong (https://twitter.com/AGWilliamTong)**
Facebook: **CT Attorney General (https://www.facebook.com/CTAttorneyGeneral/)**

Media Contact:

Elizabeth Benton
elizabeth.benton@ct.gov (mailto:elizabeth.benton@ct.gov)

Consumer Inquiries:

860-808-5318
attorney.general@ct.gov (mailto:attorney.general@ct.gov)