

Blackbaud Fined \$3M For 'Misleading Disclosures' About 2020 Ransomware Attack

Cloud computing vendor Blackbaud has been slapped with a \$3 million civil penalty by the Securities and Exchange Commission (SEC) for making misleading disclosures about a 2020 ransomware attack that impacted more than 13,000 customers.

According to a statement from the SEC, the South Carolina-based Blackbaud was not forthcoming about the extent of the data-extortion malware attack and left out material information about the scope of the incident.

In July 2020, Blackbaud confirmed it made a ransom payment to help with data recovery efforts after ransomware actors infected its corporate network.

"Our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment," the company said at the time.

Blackbaud's incident notice, which has since been removed from its website, said the attackers did not access credit card data, bank account information or the social security numbers of its customers.

Now the SEC says it found Blackbaud's claim that the

ransomware attacker did not access donor bank account information or social security numbers to be misleading.

From the SEC statement:

“Within days of these statements, however, the company’s technology and customer relations personnel learned that the attacker had in fact accessed and exfiltrated this sensitive information. These employees did not communicate this information to senior management responsible for its public disclosure because the company failed to maintain disclosure controls and procedures.

Due to this failure, in August 2020, the company filed a quarterly report with the SEC that omitted this material information about the scope of the attack and misleadingly characterized the risk of an attacker obtaining such sensitive donor information as hypothetical.”

“Blackbaud failed to disclose the full impact of a ransomware attack despite its personnel learning that its earlier public statements about the attack were erroneous,” said David Hirsch, Chief of the SEC Enforcement Division’s Crypto Assets and Cyber Unit, noting that Blackbaud failed in its obligation to provide their investors with accurate and timely material information.

Without admitting or denying the SEC’s findings, Blackbaud agreed to cease and desist from committing violations and pay a \$3 million civil penalty.

Related: Blackbaud Says Bank Account Data, SSNs Impacted in Ransomware Incident

Related: Cloud Company Blackbaud Pays Ransomware Operators to Avoid Data Leak

Related: FBI Warns of NetWalker Ransomware Targeting Businesses

Related: Law Enforcement, Cyber Insurance Powering Anti-Ransomware Success

Blackbaud Fined \$3M For 'Misleading Disclosures' About 2020 Ransomware Attack