AIDS Foundation Chicago Confirms Donor Data Breach Via Third Party

The cybercriminal did not access Social Security or credit card numbers or banking information.

August 6, 2020 By Trent Straube

AIDS Foundation Chicago (AFC) emailed people who have a history with the organization to inform them that a cybercriminal had accessed and copied a file of AFC data in a ransomware attack.

“It’s important to note that the cybercriminal did not access your credit card information, bank account information or Social Security Number,” read the notice, signed by AFC president and CEO John Peller. “However, we have determined that the file…may have contained your contact information, demographic information, and a history of your relationship with our organization, such as donation dates and amounts.”

The data breach occurred at Blackbaud, a company that provides database systems to AFC among numerous other foundations, health care organizations and nonprofits. It specializes in cloud software and services as well as data intelligence.

Ransomware is a type of malware attack in which the cybercriminal locks users out of a system and demands a ransom to grant them access back into it.

“Though we have no reason to believe your data has been or will be misused,” the AFC notice continued, “we are notifying you as a best practice, and so that you can take additional steps to protect yourself.”

The email directed anyone with further concerns to contact AFC at 312-922-2322 or info@aidschicago.org.

Here is how Blackbaud describes the security incident:

> In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, 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 cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. This incident did not involve solutions in our public cloud environment (Microsoft Azure, Amazon Web Services), nor did it involve the majority of our self-hosted environment. The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.
