Société Alzheimer Society
NOVA SCOTIA

Blackbaud Database Breach F.A.Q's

When did ASNS find out?

We found out in late July. Blackbaud emailed clients to tell them about the data breach, ASNS had to investigate whether our database was breached specifically. After consulting Blackbaud it was confirmed that our back up of our data base, between February and May, was breached.

Who is Blackbaud?

Blackbaud is a cloud computing provider that serves the social good community — non-profits, foundations, corporations, education institutions, healthcare organizations, religious organizations, and individual change agents.

After learning about various databases, ASNS chose Blackbaud's E-tapestry product in 2012. The Alzheimer Society of Nova Scotia uses this database to manage donor, client, volunteer, and partnership, information

ASNS does not keep credit card information in our database. We do not have access to anyone's health/medical records.

What happened?

(this is the answer from Blackbaud)
The Cybercrime industry represents an over trillion-dollar industry that is ever-changing and growing all the time—a threat to all companies around the world. At Blackbaud, our Cyber Security team successfully defends against millions of attacks each month and is constantly studying the landscape to ensure we are able to stay ahead of this sophisticated criminal industry.

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 attempted 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 or bank account information. Because protecting our customers' data was 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. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organisations whose data was part of this incident and are providing resources and tools to help them assess this incident.

How does Blackbaud know that the information was not passed on to other criminals or the dark web?

Through their investigation and consultation with law enforcement, including the FBI, it was determined that the main goal of the cybercriminals was to extract a ransom from Blackbaud (which they did) and not to use the data in any other way. Blackbaud has provided assurances that they continue to monitor the dark web, in collaboration with law enforcement globally, to ensure that the compromised data is not circulating.

What is ASNS doing about this data breach?

Immediately upon notification ASNS:
- has been working with Blackbaud security to finalize a list of accounts that were breached.
- contacted the Office of the Information and Privacy Commissioner of Nova Scotia
- Created internal and external communications
- Sought out legal advice

Concurrently, ASNS has:
-drafted a phased approach to communicating the breach
-spoken with various other organizations (both Alzheimer Societies and others) about their data breach and response.

Will ASNS continue to use Blackbaud?

While disappointed that this breach has taken place, we are comfortable that Blackbaud and law enforcement have dealt with the situation and are still monitoring it.

How do you know this will not happen again?

We don't. Unfortunately, with the increasing sophistication of cybercriminals it is difficult to attest to complete safety of data stored anywhere. Despite that, we work continuously to ensure our protocols are best practices in terms of data protection. Blackbaud has assured the Alzheimer Society that they have addressed the vulnerabilities in their system and will continue to monitor for additional threats.

What do people in our database have to do now?

There is nothing you have to do. If you notice that you are receiving communications that are not the usual letters/organizations you subscribe too, please let us know.

If I have more questions, or I hear someone has questions/concerns, who do I speak to?

Please direct questions to Sarah Lyon, Director of Philanthropy, Alzheimer Society of Nova Scotia sarah.lyon@asns.ca / 902-229-6093.