Ronald McDonald House Charities® Manitoba

566 Bannatyne Avenue, Winnipeg, Manitoba, R3A 0G7
Tel: 204.774.4777 | Fax: 204.774.2160 | rmhcmanitoba.org

August 6, 2020

RE: NOTICE OF BLACKBAUD DATA SECURITY INCIDENT

Dear Valued Supporter*,

Ronald McDonald House Charities Manitoba (RMHC MB) is writing to advise you, as a valued supporter of RMHC MB, that one of RMHC MB's third-party service providers, Blackbaud, recently made RMHC MB aware of a data security incident that may have involved your personal information.

As RMHC MB takes the protection and proper use of your personal information very seriously, we are contacting you to make you aware of the incident, explain to you what we have been advised by Blackbaud about the incident, and to suggest steps that you may wish to consider to protect yourself in light of the incident.

Who is Blackbaud
Blackbaud is one of the world's largest software providers for non-profit organizations. Since 2010, RMHC MB has utilized its fundraising database software for recording and managing all of RMHC MB's supporter data.

What Happened
On July 16, 2020 RMHC MB was notified by Blackbaud that in May, 2020 it discovered and stopped a ransomware attack that impacted many of Blackbaud's clients worldwide, including RMHC MB. According to Blackbaud, after discovering the attack, it, together with independent forensics experts and law enforcement, successfully prevented the cybercriminal from blocking its system access and fully encrypting files; and ultimately expelled the cybercriminal from its system. However, prior to being locked out of the system, the cybercriminal was able to copy and remove a subset of data. Blackbaud has confirmed that RMHC MB data was part of the subset of data that was copied and removed.

Blackbaud also advised that it paid the cybercriminal's demand for a ransom in order to obtain confirmation that the data that had been copied and removed had been destroyed. According to Blackbaud, based upon the nature of the incident, its research and third party (including law enforcement) investigation, there is no reason to believe the data that was copied and removed went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. It also advised that, as an extra precautionary measure, it had retained third-party experts to monitor the dark web for any usage or sale of the data.

What Information Was Involved
Blackbaud has determined that the data copied and removed was primarily contact information (name, address, phone number, email) and relationship history, such as donation dates and amounts.

Blackbaud has also determined that the data that was copied and removed did not include any credit card information, bank account information or social insurance numbers. In terms of RMHC MB supporters, RMHC MB can confirm that none of your credit card information, bank account information or social insurance numbers were compromised in the incident. RMHC MB considers credit card information, bank account information and social insurance numbers as highly sensitive and therefore does not store such information anywhere on the Blackbaud system.

What We Are Doing
RMHC MB takes the security of the personal information entrusted to it by its supporters very seriously. That is the primary reason we felt compelled to make you aware of this incident involving our third-party service provider, Blackbaud.

While Blackbaud is already implementing changes to its security measures and strengthening its defenses, RMHC MB is working with Blackbaud to implement additional measures to ensure the safety and security of RMHC MB supporter data on the Blackbaud system. RMHC MB is also reviewing its other current safety and security protocols and procedures with the intent to implement such additional measures as are deemed warranted.

RMHC MB is also currently working with outside legal counsel to identify what, if any, privacy reporting obligations that it may have to regulatory authorities.

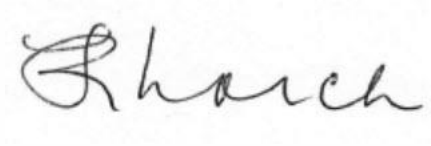
What You Can Do
While Blackbaud has advised RMHC MB that it has no reason to believe the data that was copied and removed went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly, in an effort to minimize any potential harm to you, RMHC MB is recommending that, as a precautionary and preventative measure, you closely monitor your financial and other accounts. We encourage you to set up text or other email alerts and also enroll in notifications for real-time transaction alerts via mobile apps. If you detect any unusual or suspicious activity, or if you notice any activity that you do not recognize, promptly notify the financial institution or company maintaining the account. You should also promptly report any fraudulent activity or any suspected incident of identity theft to the proper law enforcement authorities.

Also, as the data that was copied and removed was primarily contact information and relationship history, such as donation dates and amounts, there is the risk of someone impersonating RMHC MB to solicit funds. As such, you should be alert to any suspicious emails or other communications that claim to be from RMHC MB. If you have any doubt about the authenticity of any communications you should contact RMHC MB before acting.

For More Information
RMHC MB sincerely apologizes to you, our supports, for this incident and regrets any inconvenience it may cause you. You are encouraged to visit our website for additional updates as available. Should you have any questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at info@rmhmanitoba.org or 204-774-4777 ext. 224.

Sincerely,

Wendy Galagan, CEO
Ronald McDonald House Charities Manitoba



Rhonda Lorch, Board President
Ronald McDonald House Charities Manitoba

***Please note that even though you may be on the RMHC MB 'Do Not Contact' list, you are receiving this notification because it was important that you be made aware that some of your personal information may have been compromised in the incident referred to in this notice. Unless there is a subsequent update that we feel is of similar importance we will continue to honour your 'Do Not Contact' preference.**