Ronald
McDonald
House®
Dallas

Notice Regarding the Blackbaud Security Incident

Dear Friends of Ronald McDonald House of Dallas,

Ronald McDonald House Dallas ("RMHD") takes the privacy and security of the information we hold very seriously. We are reaching out regarding a data security incident at Blackbaud, a third-party software company that provides services to thousands of schools, foundations, and nonprofits, including RMHD, and is one of the world's largest providers of customer relationship management software.

Blackbaud notified its clients, including RMHD, that it had discovered and stopped a ransomware attack in May 2020. Blackbaud shared that after discovering the attempted attack, their Cyber Security team – together with independent forensics experts and law enforcement – secured their systems and began an investigation. Through the investigation, Blackbaud determined that an unauthorized person obtained access to its network between February 7, 2020 and May 20, 2020, and during that time, backup files containing information belonging to Blackbaud's clients had been taken. Blackbaud paid a ransom and obtained confirmation that the files that had been removed, had been destroyed.

Further details regarding the incident are available at https://www.blackbaud.com/securityincident.

Upon learning of the incident from Blackbaud, we immediately conducted our own investigation to understand the extent of the incident and to determine what information may have been involved.

We determined that the backup file involved may have contained information pertaining to our guests and their families and guardians. The information varied by individual, but generally included names, dates of birth, drivers' license or state ID numbers, passport numbers, visas, or other government issued identification numbers. For some individuals, the information also included limited clinical or treatment information, such as healthcare provider names and/or diagnoses information. Importantly, credit card information was not involved in this incident. Additionally, we do not collect other financial account information as part of our guest services.

Blackbaud assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe that any data was or will be misused or disseminated publicly. However, as a precaution, we are mailing letters to individuals notifying them of the incident and providing additional information on identity theft prevention. It is always a good idea to remain vigilant for incidents of fraud or identity theft be reviewing account statements for any unauthorized activity. Additional information on steps you can take to monitor and protect your information are available at ftc.gov/idtheft.

Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data from any subsequent incidents, and are undertaking additional efforts to enhance their security processes. At RMHD, we no longer use Blackbaud to manage our guest services, and are also reviewing how information is stored with third-party vendors, including Blackbaud.

We value your privacy and deeply regret that this incident occurred. We thank you for your patience and understanding and for your continued support of our mission. We have established a dedicated, toll-free call center to answer questions individuals may have. If you have questions or do not receive a letter but think your information may have been involved, please call 1-800-773-6682, Monday through Friday, from 8:00 am to 5:00 pm, Central Time. You can also contact us at house@rmhdallas.org.

Sincerely,

Jill Cumnock
Chief Executive Officer