APPENDIX

Ronald McDonald House of Dallas ("RMHD") was notified by Blackbaud, Inc. ("Blackbaud"), a third-party fundraising software provider used worldwide by thousands of nonprofits, foundations, and others, including RMHD, of a ransomware attack on Blackbaud's network that it discovered in May of 2020. Blackbaud reported that it conducted an investigation of the incident and determined that that an unauthorized person obtained access to its network between February 7, 2020 and May 20, 2020, and backup files containing information from some of its clients had been taken from its network. Blackbaud paid a ransom and obtained confirmation that the stolen files had been destroyed. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, RMHD conducted its own investigation of the Blackbaud services it uses to determine what information may have been involved in the incident. RMHD determined that a backup of the database previously used to manage RMHD's guest services may have been accessed or acquired by the unauthorized person. RMHD determined that the backup file involved may have contained the personal information of two Maine residents, including their name and one or more of the following: driver's license or state ID number, passport number, and/or other government issued identification number. Importantly, Blackbaud assured RMHD that credit card information was not involved in this incident. Additionally, RMHD does not collect other financial account information as part of its guest services.

On January 14, 2021, RMHD will begin mailing notification letters to the Maine residents via First Class US Mail. A copy of the notification letter is enclosed.[1] RMHD is offering individuals with an impacted driver's license or state ID number a complimentary one-year membership to credit monitoring and identity theft protection services through Experian. RMHD has also established a dedicated, toll-free number for individuals to obtain more information regarding this incident.

Blackbaud informed RMHD that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data, and are undertaking additional efforts to improve the security of its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms. Additionally, RMHD no longer uses Blackbaud to manage its guest services and is also reviewing how information is stored with third-party vendors, including Blackbaud.

[1] This notice does not waive RMHD's objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.

Ronald McDonald House of Dallas
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

Ronald McDonald House Dallas
Keeping families close™

[redacted]

A-8568

January 11, 2020

Dear [redacted]:

We are writing to inform you about a security incident involving Blackbaud, a third-party software company that provides services to thousands of schools, foundations, and nonprofits, including Ronald McDonald House of Dallas ("RMHD"). This notice explains the incident, outlines the measures taken in response, and provides steps you can take.

What Happened?
Blackbaud informed us that it had experienced a security incident that may have involved unauthorized access to a backup of the database we previously used to manage our guest services. Blackbaud reported that it worked with security experts and law enforcement to conduct an investigation into the incident. Through the investigation, Blackbaud determined that an unauthorized person obtained access to its network between February 7, 2020 and May 20, 2020, and that backup files containing information from its clients had been taken from its network. Blackbaud paid a ransom and obtained confirmation that the files that had been removed, had been destroyed.

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.

What Information Was Involved?
We determined that the backup file involved may have contained your name and one or more of the following: driver's license or state ID number, passport number, visa, and/or other government issued identification number. Importantly, Blackbaud assured us that credit card information was not involved in this incident. Additionally, we do not collect other financial account information as part of our guest services.

What We Are Doing.
We are notifying you of this incident and sharing the steps that we, and Blackbaud, are taking in response. 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.

What You Can Do.
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, we wanted to notify you of this incident to assure you we take this very seriously. As a precaution, we are offering a complimentary one-year membership of Experian's IdentityWorks^{SM} Credit 3B. This product helps detect possible misuse of your personal information and provides identity protection services focused on identification and resolution of identity theft. IdentityWorks^{SM} Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks^{SM} Credit 3B, including instructions on how to activate your complimentary membership, please see the additional information provided with this letter.

For More Information.

We regret that this occurred and apologize for any inconvenience this may cause. Should you have any further questions regarding this matter, please do not hesitate to call 1-800-773-6682, Monday through Friday, between 8:00 am and 5:00 pm Central Time.

Sincerely,

Jill Cumnock
Chief Executive Officer

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **March 21, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **March 21, 2021**. Be prepared to provide engagement number **B007888** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: Ronald McDonald House of Dallas is located at 4707 Bengal St, Dallas, TX, 75235 and can be reached at (214) 631-7354. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.