McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

January 18, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Houston SPCA and The Wildlife Center of Texas – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Houston SPCA and The Wildlife Center of Texas ("Houston SPCA"). I am writing to provide notification of an incident at Blackbaud, Houston SPCA's third-party software and service provider, that may affect the security of personal information of approximately three (3) New Hampshire residents. Houston SPCA's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Houston SPCA does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 16, 2020, Blackbaud notified Houston SPCA of a security incident that impacted its clients across the world. Blackbaud reported to Houston SPCA that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed Houston SPCA that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020.

Once Houston SPCA was informed of the issue, Houston SPCA immediately initiated an internal investigation. As a part of its investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, Houston SPCA engaged outside experts experienced in handling these types of incidents to help determine the impact to its stakeholders and appropriately notify them. On December 18, 2020, Houston SPCA determined that the information removed by the threat actor may have contained a limited amount of personal information, including full names and financial account numbers.

According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed, and there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud also indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity. Nevertheless, out of an abundance of caution, Houston SPCA wanted to

inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Houston SPCA is providing the affected residents with written notification of this incident commencing on or about January 19, 2021, in substantially the same form as the letter attached hereto. Houston SPCA is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are being advised to review their financials and notify their financial institutions of suspicious activity. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Houston SPCA, protecting the privacy of personal information is a top priority. Houston SPCA remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Blackbaud has assured Houston SPCA that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. Houston SPCA continually evaluates and modifies its practices, and those of its third party service providers, to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Dominic A. Paluzzi

Encl.

HOUSTON SPCA

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

[redacted]

[redacted]

Thank you for all that you've done for the Houston SPCA and our mission to help the pets and wildlife we both love. As a trusted donor of this organization, the privacy and security of the personal information we maintain as part of donation gift processing is of the utmost importance to Houston SPCA and The Wildlife Center of Texas. Today, we are writing with important information regarding a data security incident at Blackbaud. Blackbaud is a software and service provider that serves over 45,000 nonprofits worldwide and maintains millions of donor records. As a Blackbaud application client, we were informed about a possible security breach in limited fields of the data storage system we use to help us fulfill our mission. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect you.

What Happened?

On July 16, 2020, Blackbaud notified their clients of a security incident that impacted thousands of nonprofits worldwide. Blackbaud reported to all their clients that they identified an attempted ransomware attack while it was in progress on May 20, 2020. **Blackbaud informed us that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020, and May 20, 2020. According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed.**

What We Are Doing.

Once we were informed of the issue, we immediately initiated our internal investigation. As part of our investigation, we worked with Blackbaud to obtain specific information about the incident's nature and scope. We engaged outside experts experienced in handling these types of incidents. To date, we have no reason to believe that Blackbaud's information was inaccurate, and we have not discovered any compromised data or donor information. But, in an abundance of caution, we think informing you, our valuable donors, of the possibility, is the correct course of action.

What Information Was Involved.

Beginning September 25, 2020, we launched our extensive investigation, which concluded on December 18, 2020. At such time, we determined that the information removed by the threat actor may have contained some personal information, including your full name, donation history, and financial account numbers. **We determined that NO Social Security numbers, credit card information, or any online donations were exposed because of this incident.**

What You Can Do.

According to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a group of forensics accountants, to continue monitoring for any such activity. Like all of us in a world that data breaches are becoming more common, we know you will always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity regularly and report any suspicious activity to the proper authorities. If, in reviewing your financials for the year, you feel there is any suspicious activity especially between February 2020 and May 2020, please contact your financial institution and let them know.

For More Information.

We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Blackbaud has assured us that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. We continually evaluate and modify our practices and those of our third-party service providers to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please contact [redacted] at [redacted].

We cannot do the work we do without you. Your generosity and love of all the animals and wildlife that we help make our lifesaving programs possible. Thank you for walking with us as we continue to serve pets, farm animals and, equine in our community.

Sincerely,

[redacted]

Houston SPCA and The Wildlife Center of Texas

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "fraud alert" on your credit files at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account, or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts.

You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.