



September 18, 2020

Hunter O. Ferguson  
600 University Street, Suite 3600  
Seattle, WA 98101  
D. 206.386.7514  
hunter.ferguson@stoel.com

**VIA EMAIL SECURITYBREACH@ATG.WA.GOV**

Attorney General Bob Ferguson  
Office of the Attorney General  
1125 Washington Street SE  
PO Box 40100  
Olympia, WA 98504-0100

**Re: Notice of Data Security Incident**

Dear Attorney General Ferguson:

We are writing on behalf of our client, Homeward Pet Adoption Center (“*Homeward Pet*”) to notify you of a security incident involving a service provider engaged by Homeward Pet – Blackbaud, Inc. (“*Blackbaud*”) – that involved the disclosure of personal information of Washington residents requiring notice under RCW 19.255.010(5), namely individuals’ names and dates of birth. Homeward Pet is a non-profit organization based in Woodinville, Washington, devoted to caring for and pairing pets with families. Homeward Pet, like many non-profit organizations, uses Blackbaud as a service provider to process donations and manage donor records.

1. Nature of the Incident

As you are likely familiar, in light of the publicity of the Blackbaud incident and the notices that your office has already received about the underlying incident, Blackbaud is one of the largest donor management software companies serving non-profits, including Homeward Pet. Blackbaud notified Homeward Pet on July 16, 2020 that it experienced a data breach between February 7, 2020 and May 20, 2020. This breach affected numerous non-profits Homeward Pet, nationally and internationally. As part of the breach, the cybercriminal accessed or might have been able to access a backup file (the “*accessed file*”) containing personal information of Washington residents that Homeward Pet had uploaded to the Blackbaud service.

2. Number of Affected Washington Residents and Types of Compromised Personal Information

After receiving notice of the incident, Homeward Pet investigated what information had been supplied to Blackbaud for processing and determined that the accessed file included personal information of 36,050 Washington residents (out of 38,709 individuals total). The personal information involved included the Washington resident's names, addresses, email addresses, telephone numbers, their relationship with Homeward, past donations, and dates of birth.

Blackbaud informed Homeward Pet that it engaged forensic experts and law enforcement to assist in the investigation and containment of the breach. Blackbaud also informed Homeward Pet that it believes the cybercriminal destroyed the personal information and that Blackbaud has no reason to believe that the data will be misused further or that the cybercriminal shared the data before destroying it.

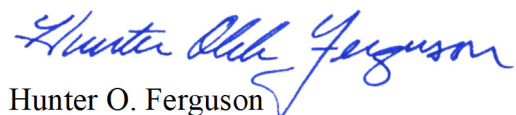
3. Actions Homeward Pet Is Taking

On September 18, 2020, Homeward Pet sent the enclosed email notice to all of its donors. Homeward Pet regularly communicates with its donors via email, and this email notice contains a link to a new page on Homeward pet's website detailing the incident and advising individuals how to protect their information (<https://www.homewardpet.org/uncategorized/steps-you-can-take-to-further-protect-your-information/>). Homeward Pet is also in the process of mailing to its donors via U.S. Mail the enclosed notice, which is identical to the email/website notice and explains what happened in the incident, what personal information was involved, what further steps Homeward Pet took in response to the incident, and what individuals can do to protect their information. All of these paper notices should be mailed by September 25.

Although the breach involved Blackbaud's network, not the networks of Homeward Pet, Homeward Pet is taking this opportunity to evaluate security protocols and reinforce staff education about security.

For further information or if you have any questions regarding this notice, please contact me at 206.386.7514 or by email at [hunter.ferguson@stoel.com](mailto:hunter.ferguson@stoel.com)

Very truly yours,

  
Hunter O. Ferguson

Enclosures



## A NOTE FROM NANETTE MCCANN, EXECUTIVE DIRECTOR....

To Our Friends and Donors:

We are writing to inform you of a recent cybersecurity incident that may have involved some of your personal information.

Earlier this year, criminals engineered a “ransomware attack” against Blackbaud—one of the largest software service providers that supports nonprofits, including Homeward Pet Adoption Center. During this incident, criminals gained access to Blackbaud’s systems and made many of its data files unusable. Fortunately, your financial account and credit/debit card information were not accessible in this incident, but there is a possibility that other information—such as names, contact information, and birthdays—was accessible. **Please [click here](#) to learn more and what you can do to protect your information.**

Our network and systems were not affected by this incident, and we have not received any indication that any information regarding our friends or donors has been misused or was even actually accessed in the incident. Nevertheless, out of an abundance of caution and in the interest of transparency, we are notifying you. We are also in the process of mailing notices to our friends and donors using addresses we have on file, so you may receive a follow-up notice in the mail.

We apologize for this incident. If you have any questions, please do not hesitate to contact me at [nanette@homewardpet.org](mailto:nanette@homewardpet.org).

Sincerely,

A handwritten signature in black ink that reads "Nanette McCann". The signature is written in a cursive, flowing style.

Nanette McCann  
Executive Director  
Homeward Pet Adoption Center

Homeward Pet Adoption Center  
P.O. Box 2293  
13132 NE 177th Pl  
Woodinville, WA 98072



[DATE]  
[Primary Addressee]  
[Address]  
[City], [State ZIP]

## NOTICE OF DATA BREACH

Dear [Name],

We are writing to let you know about a data security incident that may have involved your personal information. Homeward Pet takes the protection and proper use of your information very seriously. Therefore, we are contacting you to explain the incident and provide you with steps you can take to protect yourself.

### **What Happened**

We were recently notified of a cybersecurity incident by one of our service providers, Blackbaud, Inc. We use Blackbaud's services to process donations to our organization and to help manage our donor records. According to Blackbaud, it suffered a ransomware attack in which a cybercriminal gained access to its computer network and files and tried to prevent Blackbaud from using its data files. Blackbaud informed us that, as part of this incident, the cybercriminal may have been able to access files that contained some of your personal information, although there is not a clear indication that an unauthorized user actually accessed your information. Blackbaud has reported that, with the help of cybersecurity experts and law enforcement, it ultimately expelled the cybercriminal from its systems.

According to Blackbaud, this incident occurred on February 7, 2020, and the criminal could have accessed their system until May 20, 2020.

### **What Information Was Involved**

It's important to note that the cybercriminal did not access your credit card information, bank account information, or social security number. Blackbaud explained that this information was encrypted, so the cybercriminal was not able to access it. However, we have determined that the file removed may have contained your contact information, demographic information (age, date of birth, marital status), and a history of your relationship with our organization, such as donation dates and amounts.

Blackbaud paid the cybercriminal's demand and received confirmation that the

data copy they removed had been destroyed. Based on the nature of the incident, their 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.

### **What We Are Doing**

We are continuing to monitor reports and gather other information about the incident. The incident did not involve our systems, but we are examining our security and other ways to protect your data, such as evaluating how we collect and store personal information. Although we are not certain that the cybercriminal accessed your information in particular, we are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of our constituents' data is of the utmost importance to us.

As part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has advised us that it has implemented several changes that will protect your data from any subsequent incidents. According to Blackbaud, it was able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. Blackbaud reports that it has confirmed, through testing by multiple third parties, including the appropriate platform vendors, that its security improvements withstands all known attack tactics. Additionally, Blackbaud has stated that it is accelerating efforts to further improve its security by enhancing its system access management, network segmentation, and deployment of additional endpoint and network-based platforms.

### **What You Can Do**

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. Please review the attachment to this letter ("Steps You Can Take to Further Protect Your Information") for further information on actions you can take to protect yourself.

### **For More Information**

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact me at (425) 488-4444 ext. 4005 or [nanette@homewardpet.org](mailto:nanette@homewardpet.org).

Sincerely,

A handwritten signature in black ink, appearing to read "Nanette McCann". The signature is fluid and cursive, with the first name "Nanette" written in a larger, more prominent script than the last name "McCann".

Nanette McCann  
Executive Director  
107991641.1 0099880-01350

## **Steps You Can Take to Further Protect Your Information**

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax  
(800) 685-1111  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

Experian  
(888) 397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 4500  
Allen, TX 75013

TransUnion  
(888) 909-8872  
[www.transunion.com](http://www.transunion.com)  
2 Baldwin Place  
P.O. Box 1000  
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>.

- **Security Freeze**

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check.

Contact the three credit reporting agencies listed above (Equifax, Experian and TransUnion) to request a security freeze. The credit reporting agencies' websites explain how to request a security freeze. *You must separately place a security freeze on your credit file with each credit reporting agency.*

To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.