Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 11, 2021

VIA E-MAIL

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
E-mail: ndag@nd.gov

Re: Notice of the Blackbaud Data Event

Dear Sir or Madam:

We represent the Alzheimer's Association located at 225 N. Michigan Ave. Floor 17, Chicago, IL 60601, and are writing to notify your office of an incident that may affect the security of some personal information relating to four thousand seven hundred fifty-eight (4,758) North Dakota residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Alzheimer's Association does not waive any rights or defenses regarding the applicability of North Dakota law, the applicability of the North Dakota data event notification statute, or personal jurisdiction.

Nature of the Data Event

Blackbaud is a cloud computing provider that provides financial services tools to Alzheimer's Association. On July 16, 2020, Alzheimer's Association received notification from Blackbaud of a cyber incident that occurred on Blackbaud's network. According to Blackbaud, in May 2020 they discovered and stopped a ransomware security incident. With support of forensic specialists and law enforcement, Blackbaud represented that it successfully blocked the ransomware incident. However, Blackbaud reported the threat actor was able to exfiltrate data from Blackbaud's network before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until two months later on July 16, 2020 that Blackbaud notified Alzheimer's Association that an unknown actor may have accessed or acquired certain Blackbaud customer data.

Upon receiving notice from Blackbaud, Alzheimer's Association immediately investigated this incident the nature and scope of the incident and any impact on Alzheimer's Association data. This investigation included working diligently to gather additional information from Blackbaud to understand the scope of the incident. On or about August 5, 2020, Alzheimer's Association received further information from Blackbaud that could not rule out unauthorized access to Alzheimer's Association databases that contained personal information. Because of Blackbaud's disclosures, Alzheimer's Associations conducted a

comprehensive review of the impacted databases with assistance from third-party specialists to identify the individuals whose personal information was potentially accessible. While this review was ongoing, on October 6, 2020, Blackbaud notified Alzheimer's Association of additional database information that may have been impacted, expanding the scope of the review. On December 3, 2020, Alzheimer's Association completed the comprehensive review and confirmed the impacted databases included personal information defined by N.D. Cent. Code Ann. § 51-30-01 for four thousand seven hundred fifty-eight (4,758) North Dakota residents, including name, address, date of birth, Social Security number, financial account number, and medical information.

Notice to North Dakota Residents

From December 30, 2020 through January 11, 2021, Alzheimer's Association provided notice of this incident to potentially affected individuals including four thousand seven hundred fifty-eight (4,758) North Dakota residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Alzheimer's Association moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included extensive coordination with Blackbaud to confirm what information could have been potentially affected that may have contained personal information. Alzheimer's Association is working to review existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. Alzheimer's Association is providing access to credit monitoring services for 12 months, through TransUnion and Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Alzheimer's Association is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Alzheimer's Association is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/dle

Exhibit A

alzheimer's association

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

225 N. Michigan Ave., Fl. 17
Chicago, IL 60601
alz.org
800-272-3900
312-335-8700 p
866-699-1246 f

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF BLACKBAUD DATA <<VARIABLE DATA 2>>

Dear <<Name 1>>:

The Alzheimer's Association is deeply dedicated to all constituents we serve and appreciates the generosity of our donors. In an effort to share information and foster relationships that support the important mission of the Alzheimer's Association, we partner with Blackbaud, an external vendor, for nonprofit software support. Regrettably, Blackbaud had a data incident that may have included some of your personal information.

What Happened

According to Blackbaud, in May 2020 they discovered and stopped a ransomware security incident. With support of forensic specialists and law enforcement, Blackbaud represented that it successfully blocked the cyber-attack, preventing access to the entire system or to fully encrypted files. Unfortunately, the company reported that information contained on specific Blackbaud systems was exposed between May 14, 2020, and May 20, 2020. Blackbaud notified the Alzheimer's Association on July 16, 2020, two months later.

After being informed of Blackbaud's data event, we immediately sought to determine the nature and scope of any impact to our data. This investigation included working diligently to gather additional information from Blackbaud.

On December 3, 2020, we completed the comprehensive review and identified the individuals and their data that was maintained in the potentially impacted databases.

What Information Was Involved

Your personal information maintained on the impacted portion of Blackbaud's network consisted of your first and last name and the following: <<Data Elements>>. At this time, we have no evidence of any misuse of any personal information.

What We Are Doing

As noted above, once notified by Blackbaud, we immediately initiated an independent investigation. As part of our ongoing commitment to the security of personal information in our care, we are holding Blackbaud accountable to evaluate additional measures and safeguards to protect against this type of incident in the future.

We are also working to determine why Blackbaud did not notify us sooner and why Blackbaud did not provide the full scope of potentially impacted data in its initial notification. We are also reviewing our policies and procedures for third-party vendors to ensure all safeguards for privacy and security are in place.

Additionally, we are notifying potentially impacted individuals and providing guidance as to steps individuals may take to protect their information.

As an added precaution, we are offering access to identity monitoring and identity theft protection services without cost to you for 12 months. Enrollment instructions are included in the "Steps You Can Take to Protect Your Personal Information" section of this letter. We encourage you to enroll in these services as we are unable to do so on your behalf.

What You Can Do

Enclosed is "Steps You Can Take to Protect Your Personal Information," which describes steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

We sincerely regret any inconvenience or concern this incident may cause and understand that you may have questions. If you have questions, please call our dedicated assistance line at 800-923-5048 (toll free), Monday through Friday from 9:00 AM to 9:00 PM Eastern Time (excluding U.S. holidays). You may also write to the Alzheimer's Association at 225 N. Michigan Ave, Fl. 17, Chicago, IL 60601.

Thank you for your commitment to the mission of the Alzheimer's Association.

Sincerely,

Richard H. Hovland
Chief Operating Officer
Alzheimer's Association

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Complimentary Identity Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<6-digit Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious charges. Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-alerts

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, you may contact the Attorney General by mail, phone, or website. You may also obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. Mail: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; Phone: 1-410-528-8662; Website: www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act ("FCRA"). Those rights include but are not limited to 1) the right to be told if information in your credit file has been used against you; 2) the right to know what is in your credit file 3) the right to ask for your credit score; and 4) the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies must 1) correct or delete inaccurate, incomplete, or unverifiable information; and 2) limit access to your file; and 3) get your consent for credit reports to be provided to employers. Additionally, consumer reporting agencies may 1) not report outdated negative information; and 2) limit "prescreened" offers of credit and insurance you receive based on information in your credit report. You may also seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, you may contact the Attorney General by mail, phone, or website. You may also obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. Mail: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; Phone: 1-800-771-7755; Website: https://ag.ny.gov/.

For District of Columbia residents, you may contact the Attorney General by mail, phone, or email. You may also obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. Mail: 441 4th St. NW #1100 Washington, D.C. 20001; Phone: 1-202-727-3400; Email: oag@dc.gov.

alzheimer's association

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

225 N. Michigan Ave., Fl. 17
Chicago, IL 60601
alz.org
800-272-3900
312-335-8700 p
866-699-1246 f

<<Mail ID>>
Parent or Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF BLACKBAUD DATA <<VARIABLE DATA 2>>

Dear Parent or Guardian of <<Name 1>>:

The Alzheimer's Association is deeply dedicated to all constituents we serve and appreciates the generosity of our donors. In an effort to share information and foster relationships that support the important mission of the Alzheimer's Association, we partner with Blackbaud, an external vendor, for nonprofit software support. Regrettably, Blackbaud had a data incident that may have included some of your minor child's personal information.

What Happened

According to Blackbaud, in May 2020 they discovered and stopped a ransomware security incident. With support of forensic specialists and law enforcement, Blackbaud represented that it successfully blocked the cyber-attack, preventing access to the entire system or to fully encrypted files. Unfortunately, the company reported that information contained on specific Blackbaud systems was exposed between May 14, 2020, and May 20, 2020. Blackbaud notified the Alzheimer's Association on July 16, 2020, two months later.

After being informed of Blackbaud's data event, we immediately sought to determine the nature and scope of any impact to our data. This investigation included working diligently to gather additional information from Blackbaud.

On December 3, 2020, we completed the comprehensive review and identified the individuals and their data that was maintained in the potentially impacted databases.

What Information Was Involved

Your child's personal information maintained on the impacted portion of Blackbaud's network consisted of your child's first and last name and the following: <<Data Elements>>. At this time, we have no evidence of any misuse of any personal information.

What We Are Doing

As noted above, once notified by Blackbaud, we immediately initiated an independent investigation. As part of our ongoing commitment to the security of personal information in our care, we are holding Blackbaud accountable to evaluate additional measures and safeguards to protect against this type of incident in the future.

We are also working to determine why Blackbaud did not notify us sooner and why Blackbaud did not provide the full scope of potentially impacted data in its initial notification. We are also reviewing our policies and procedures for third-party vendors to ensure all safeguards for privacy and security are in place.

Additionally, we are notifying potentially impacted individuals and providing guidance as to steps individuals may take to protect their information.

As an added precaution, we are offering access to credit monitoring and identity theft protection services without cost to you for 12 months. Enrollment instructions are included in the "Steps You Can Take to Protect Personal Information" section of this letter. We encourage you to enroll your child in these services as we are unable to do so on their behalf.

What You Can Do

Enclosed is "Steps You Can Take to Protect Personal Information," which describes steps you can take to help protect your child's information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze.

For More Information

We sincerely regret any inconvenience or concern this incident may cause and understand that you may have questions. If you have questions, please call our dedicated assistance line at 800-923-5048 (toll free), Monday through Friday from 9:00 AM to 9:00 PM Eastern Time (excluding U.S. holidays). You may also write to the Alzheimer's Association at 225 N. Michigan Ave, Fl. 17, Chicago, IL 60601.

Thank you for your commitment to the mission of the Alzheimer's Association.

Sincerely,

Richard H. Hovland
Chief Operating Officer
Alzheimer's Association

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for your child to receive identity monitoring, at no cost, through Equifax. Equifax Child Identity Monitoring will scan the Equifax credit database for any instances of the minor's social security number and look for a copy of the minor's Equifax credit file.

- If no SSN match is found and no Equifax credit file exists, Equifax will create an Equifax credit file in the minor's name and immediately "lock" the Equifax credit file. This will prevent access to the minor's Equifax credit file in the future. If Equifax receives a request for your minor's Equifax credit report, you will receive an email alert.
- If there is a match and an Equifax credit file exists, Equifax will immediately "lock" the file and alert you to activity against the file, such as an attempt to open a new line of credit.
- The minor's Equifax credit file will be locked for 12 months from date of activation. After that time, the minor's Equifax credit file will be deleted from our credit database if it contains no credit data.

Enrollment Instructions

To enroll in Equifax Child Identity Monitoring go to http://myservices.equifax.com/efx1_brminor and follow the instructions below:

1. **Welcome Page:** Enter your unique Activation Code **<<Insert Code>>** and click the "Submit" button.
2. **Register:** Complete the form with **YOUR** contact information first (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept the Terms of Use and click the "Continue" button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.
6. **Click the orange button "Enroll Child"** to enter your child's information (child's name, Date of Birth and Social Security Number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to remove the minor from the account. You may then re-enroll the minor with the correct SSN.
7. **Check the box confirming you are the child's parent or guardian**.
8. **Click "Submit"** to enroll your child.

Monitor Accounts

Typically, a minor under the age of eighteen does not have credit in his or her name, and the consumer reporting agencies do not have a credit report in a minor's name. To find out if your minor has a credit report or to request a manual search for your minor's Social Security number each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit the below websites:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/form-minor-child.html	P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-disputes/child-identity-theft-inquiry-form	P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 my.equifax.com/consumer-registration/UCSC/#/personal-info

Under U.S. law, individuals with credit are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of a credit report should your minor have established credit.

Adults and minors sixteen years or older have the right to place a "security freeze" on a credit report, which will prohibit a consumer reporting agency from releasing information in the credit report without express authorization. A parent or guardian also has the right to place a "security freeze" on a minor's credit report if the child is under the age of sixteen. This right includes proactively placing a "security freeze" on a minor's credit report if the minor is under sixteen years old. If the nationwide credit reporting agencies do not have a credit file on the minor, they will create one so they can freeze it. This record cannot be used for credit purposes. It is there to make sure the child's record is frozen and protected against potential identity theft and fraud. Pursuant to federal law, you cannot be charged to place or lift a security freeze on a credit report. Should you wish to place a security freeze on a credit file or proactively place a freeze on a minor's credit report, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-349-9960
www.equifax.com/personal/credit-report-services

As an alternative to a security freeze, individuals with established credit have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If the minor is a victim of identity theft, he/she is entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com/personal/credit-report-services

To request information about the existence of a credit file in your minor's name, search for your minor's Social Security number, place a security freeze on your minor's credit file, place a fraud alert on your minor's credit report (if one exists), or request a copy of your minor's credit report you may be required to provide the following information:

- A driver's license or another government issued identification card, such as a state ID card, etc.;
- proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- a copy of your minor's birth certificate;
- a copy of your minor's Social Security card;
- your minor's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- your minor's date of birth; and
- previous addresses for the past two years.

You can further educate yourself regarding identity theft prevention, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

alzheimer's association®

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

225 N. Michigan Ave., Fl. 17
Chicago, IL 60601
alz.org
800-272-3900
312-335-8700 p
866-699-1246 f

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF BLACKBAUD DATA <<VARIABLE DATA 2>>

Dear Next of Kin of <<Name 1>>:

The Alzheimer's Association is deeply dedicated to all constituents we serve and appreciates the generosity of our donors. In an effort to share information and foster relationships that support the important mission of the Alzheimer's Association, we partner with Blackbaud, an external vendor, for nonprofit software support. Regrettably, Blackbaud had a data incident that may have included some of your deceased loved one's personal information.

What Happened

According to Blackbaud, in May 2020 they discovered and stopped a ransomware security incident. With support of forensic specialists and law enforcement, Blackbaud represented that it successfully blocked the cyber-attack, preventing access to the entire system or to fully encrypted files. Unfortunately, the company reported that information contained on specific Blackbaud systems was exposed between May 14, 2020, and May 20, 2020. Blackbaud notified the Alzheimer's Association on July 16, 2020, two months later.

After being informed of Blackbaud's data event, we immediately sought to determine the nature and scope of any impact to our data. This investigation included working diligently to gather additional information from Blackbaud.

On December 3, 2020, we completed the comprehensive review and identified the individuals and their data that was maintained in the potentially impacted databases.

What Information Was Involved

Your loved one's personal information maintained on the impacted portion of Blackbaud's network consisted of your loved one's first and last name and the following: <<Data Elements>>. At this time, we have no evidence of any misuse of any personal information.

What We Are Doing

As noted above, once notified by Blackbaud, we immediately initiated an independent investigation. As part of our ongoing commitment to the security of personal information in our care, we are holding Blackbaud accountable to evaluate additional measures and safeguards to protect against this type of incident in the future.

We are also working to determine why Blackbaud did not notify us sooner and why Blackbaud did not provide the full scope of potentially impacted data in its initial notification. We are also reviewing our policies and procedures for third-party vendors to ensure all safeguards for privacy and security are in place.

Additionally, we are notifying potentially impacted individuals and providing guidance as to steps individuals may take to protect personal information.

What You Can Do

Enclosed is "Steps You Can Take to Protect Personal Information," which describes steps you can take to help protect your loved one's information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your loved one's credit file.

For More Information

We sincerely regret any inconvenience or concern this incident may cause and understand that you may have questions. If you have questions, please call our dedicated assistance line at 800-923-5048 (toll free), Monday through Friday from 9:00 AM to 9:00 PM Eastern Time (excluding U.S. holidays). You may also write to the Alzheimer's Association at 225 N. Michigan Ave, Fl. 17, Chicago, IL 60601.

Thank you for your commitment to the mission of the Alzheimer's Association.

Sincerely,

Richard H. Hovland
Chief Operating Officer
Alzheimer's Association

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Accounts

To further protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your loved one's account statements, and to monitor his or her credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

Contact information for the three consumer reporting agencies is listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com

You can also request, in writing, that the report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your loved one's name and what to do if your loved one's identity becomes subject to such fraud.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For New York residents, you may contact the Attorney General by mail, phone, or website. You may also obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. Mail: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; Phone: 1-800-771-7755; Website: https://ag.ny.gov/.

For District of Columbia residents, you may contact the Attorney General by mail, phone, or email. You may also obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. Mail: 441 4th St. NW #1100 Washington, D.C. 20001; Phone: 1-202-727-3400; Email: oag@dc.gov.