

17675



199 Water St, 11th Floor,
New York, NY 10038

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: Important Security Notification. Please read this entire letter.

Dear <<First Name>>:

We are writing to inform you of a data security incident experienced by Blackbaud, Inc. ("Blackbaud"), a provider of cloud-based data management services to American Friends of The Hebrew University ("AFHU") as well as many other not-for-profit organizations, schools, colleges and universities. According to the information provided by Blackbaud, certain information relating to AFHU donors was contained within the affected Blackbaud systems.

While we have been assured by Blackbaud that the response to the criminal activity that led to the incident was managed fully and all information compromised was destroyed, we nonetheless are sharing with you what we know as we work diligently to ensure that this incident is sufficiently addressed. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks. Nevertheless, out of an abundance of caution, we wanted to advise you of this incident.

The security of our constituents' and donors' personal information is of the utmost importance to us and we deeply regret this incident. We have made clear to Blackbaud that we expect to receive information regarding the incident and what steps were taken by Blackbaud to remediate the incident, including, but not limited to, what enhanced security practices are being put in place.

What Information Was Involved:

According to Blackbaud, bank account information, usernames, and passwords that may have been entered into the affected systems were encrypted and the decryption keys were not compromised. Therefore, it appears that this information was not subject to misuse or unauthorized disclosure. Further, **Blackbaud has stated that none of our donors' payment (credit, debit, etc.) card information was included in the compromised database and therefore was not impacted as a result of this incident.**

However, other information concerning our donors and constituents may have been acquired by the attacker. Notably, Blackbaud has not provided specific information regarding what types of data may have been impacted. Rather, Blackbaud has only provided general information regarding the databases potentially affected. Again, payment card information were not compromised. We are working diligently to obtain additional information from Blackbaud to gain a better understanding of the scope of the incident. **Currently, it is our understanding that the information potentially impacted may include your name and date of birth. Additionally, AFHU has discovered that sensitive attachments were not encrypted by Blackbaud and may contain your social security number. While Blackbaud has not confirmed that this information was in fact impacted, we are providing you with this notification, as well as complimentary credit monitoring, so that you may take steps to protect your personal information.**

What Is Being Done:

Blackbaud has indicated that they are taking efforts to further secure their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. However, Blackbaud has not provided more specific information regarding the steps taken to remediate this incident. We are working diligently to obtain additional information from Blackbaud regarding the scope of the incident and what steps have been taken to ensure that a similar incident does not occur in the future. Additionally, as stated above, we are working to obtain additional information from Blackbaud regarding what specific information may have been impacted as a result of this incident to ensure that the proper notification is provided to individuals whose sensitive information may have been impacted.

Identity Monitoring:

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online identity monitoring service for two years provided by Kroll, a data breach and recovery services expert. Due to privacy laws, we cannot activate you directly. Additional information regarding how to activate in the complimentary identity monitoring service is enclosed.

What You Can Do:

While we work to obtain additional information from Blackbaud, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to help guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, we have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information:

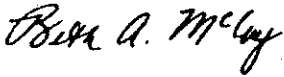
Should you have questions or concerns regarding this matter, please do not hesitate to contact Ariel Londono, Controller, at alondono@afhu.org.

AFHU has no relationship more important or more meaningful than the one we share with our donors and constituents. We deeply regret any worry or inconvenience that this incident may cause.

Sincerely,



Clive Kabatznik
President



Beth A. McCoy
CEO

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

Kroll provides you with the following features:¹

- Credit Monitoring - You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.
- \$1 Million Identity Fraud Loss Reimbursement.
- Fraud Consultation.
- Identity Theft Restoration.

How to Activate: You can sign up online.

- Visit <https://enroll.idheadquarters.com> to activate and take advantage of your complimentary credit monitoring and identity protection services.
- You have until December 7, 2020 to activate your credit monitoring and identity protection services.
- Membership number: <<Member ID>>

Due to privacy laws, we cannot activate you directly. Activating this service will not affect your credit score. Activation is available online only as no offline options are available at this time.

PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion

Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834
1-800-680-8289
www.transunion.com

Experian

National Consumer Assistance
P.O. Box 1017
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

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

PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. 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. In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: 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, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. 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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. 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.

MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to help protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at <http://www.annualcreditreport.com>. Under Rhode Island and Massachusetts law, you have the right to obtain any police report filed in regard to this incident.

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.
- **For New York residents**, 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>
- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.
- **For Rhode Island Residents**, the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov> or 401-274-4400.