McDonald Hopkins
A business advisory and advocacy law firm®

100 International Drive
23rd Floor
Baltimore, MD 21202

P: 1.410.917.5189

Spencer S. Pollock
Direct Dial: (410) 917 5189
E-mail: spollock@mcdonaldhopkins.com

November 21, 2023

VIA Online Portal

Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Big Brothers Big Sisters of America – Incident Notification

Dear Attorney General Frey:

McDonald Hopkins PLC represents Big Brothers Big Sisters of America ("BBBSA"). I am writing to provide notification of an incident at BBBSA that may affect the security of personal information of approximately 123 Maine residents. BBBSA'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, BBBSA does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

BBBSA experienced a security incident that impacted their network on or about March 28, 2023. Upon learning of this issue, BBBSA immediately contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, BBBSA engaged external cybersecurity professionals experienced in handling these types of incidents to determine the extent of any compromise of the information on the BBBSA network. Based on the comprehensive investigation, BBBSA concluded that certain documents and records maintained within their possession were accessed and/or obtained in connection with this incident. Following the extensive manual document review, BBBSA determined on November 15, 2023 that certain personal information was present in those documents and records. The impacted data includes full name in combination with Social Security number, date of birth, driver's license number and/or state identification number, payment card number, account number, account type, routing number, institution name, email address and password, medical information and health insurance information. Not all data elements were impacted for every Maine resident. On November 20, 2023, BBBSA located the most recent contact information for the impacted individuals.

To date, BBBSA is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, BBBSA is providing notice to the affected clients commencing on November 22, 2023 in substantially the same form as the

enclosed letter (Attached as Exhibit A). The notified individuals who have had their Social Security number impacted will receive complimentary credit monitoring services. Additionally, BBBSA will advise all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. BBBSA will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for BBBSA. BBBSA remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. BBBSA continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (410) 917 5189 or spollock@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Spencer S. Pollock

Encl.

Exhibit A

Big Brothers Big Sisters of America
c/o Cyberscout
[redacted]

[redacted]

Big Brothers Big Sisters.

November 22, 2023

Important Information
Please review carefully

Dear [redacted]

I am writing with important information regarding a recent data security incident that Big Brothers Big Sisters of America ("BBBSA") experienced. The privacy and security of personal information entrusted to us is of the utmost importance to BBBSA. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we are continuing to take measures to protect your information.

What Happened?

We experienced a security incident on or about March 28, 2023, that impacted our network environment. After a thorough investigation and extensive review of impacted data, we discovered on November 15, 2023, that the files the unauthorized actor downloaded contained some of your personal information. We took steps, to the best of our ability and knowledge, to ensure that the stolen data is deleted by the unauthorized actor, although we cannot guarantee this result. We want to make you aware of the incident and provide you with steps you can take to further protect your information.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked closely with external cybersecurity professionals and notified the FBI of the incident. Additionally, BBBSA is reviewing its existing policies and training protocols relating to data protection while enhancing security measures and monitoring tools to further mitigate risks of this nature. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your protected personal information.

What Information Was Involved?

The data that the unauthorized actor downloaded contained some of your protected personal information, [redacted]

What You Can Do.

We are providing you access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide twelve (12) months of alerts from the enrollment date when changes occur to your credit file. We are also providing you with proactive fraud assistance to help with any questions you might have or if you become a victim of fraud. Cyberscout will provide these services through Identity Force, a TransUnion company specializing in fraud assistance and remediation services

P 0000101102G0500

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter by February 22, 2024. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

This letter also provides other precautionary measures to protect your personal information, including placing a fraud alert and/or security freeze on your credit files and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We sincerely regret the occurrence of this incident. We are committed to maintaining the proper handling, protection, and privacy of protected personal information in our possession and have taken precautions to safeguard it.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. Representatives are available from [redacted] Eastern Time, Monday through Friday, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information.

Sincerely,

Tim Midkiff
Chief Financial and Administrative Officer
Big Brothers Big Sisters of America

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

Whether or not you choose to use the complimentary twelve (12)-month credit monitoring services, we recommend that you place an initial 90-day "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 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

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

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider 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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you will 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 you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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 TTY: 1-866-653-4261, 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.

You may also reach out to the Social Security Administration to notify them of the impact on your Social Security Number. They may be reached via the telephone by contacting the National 800 Number at 1-800-772-1213 between 8:00 a.m. – 7:00 p.m. Eastern Time, Monday through Friday. If you are deaf or hard of hearing and use TTY equipment, you can call the TTY number at 1-800-325-0778.

5. State Specific Information.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA) which include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.
There were [redacted] Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.