



Aubrey L. Weaver
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
AWeaver@constangy.com
941.875.5335

May 16, 2024

VIA ONLINE SUBMISSION

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

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP, represents Brockton Area Multi Services, Inc. (“BAMSI”), a 501(c)3 nonprofit organization founded in Brockton, Massachusetts, that provides a wide array of services to children, adults, and families. BAMSI takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of BAMSI because personal information for 15 Maine residents could have been involved in the data security incident.

1. Nature of the Security Incident

On April 14, 2023, BAMSI became aware of evidence of unusual activity on its systems. In response, BAMSI immediately took measures to secure its network, systems, and data. BAMSI also engaged independent cybersecurity experts to conduct a forensic investigation into the incident. This forensic investigation determined that certain BAMSI data may have been accessed or acquired without authorization in connection with this incident. As a result, BAMSI launched a comprehensive review of the potentially affected data, then worked diligently to validate the results and confirm addresses for potentially affected individuals in preparation for notification. These efforts concluded on April 29, 2024, and identified some personal information within the potentially affected dataset.

The potentially affected information varies for each individual, but may have included individuals’ names, date of birth, Social Security number, driver’s license or state identification card number, account number, diagnosis or treatment information, and/or health insurance information.

Attorney General Aaron Frey

May 16, 2024

Page 2

2. Number of Maine Residents Affected

BAMSI notified 15 Maine residents within the potentially affected population on May 16, 2024, via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as BAMSI discovered the unusual network activity, it took steps to secure its systems and launched an investigation to determine learn more about what happened and what information could have been affected. BAMSI has implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future. BAMSI also reported the issue to the FBI and other relevant authorities.

BAMSI has established a toll-free call center through IDX to answer questions about the incident and address related concerns. Additionally, BAMSI is providing those whose Social Security number was involved with identity protection services through IDX, A ZeroFox Company. The IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely,



Aubrey L. Weaver
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/BAMSI>

May 16, 2024

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident that may have affected your personal or protected health information. Brockton Area Multi Services, Inc. (“BAMSI”) is committed to maintaining our clients’ trust and demonstrating our commitment to the privacy and security of all information in our possession. This letter provides information about the incident and steps you can take to protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What Happened: On April 14, 2023, BAMSI became aware of unusual activity in our network. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened. This forensic investigation determined that certain BAMSI data may have been accessed or acquired without authorization in connection with this incident. As a result, we launched a comprehensive review of the potentially affected data, then worked diligently to validate the results and confirm addresses for potentially affected individuals in preparation for notification. These efforts concluded on April 29, 2024, and identified some of your information within the potentially affected dataset.

What Information Was Involved: The potentially affected information included your <<Variable Text 1: Data Elements>>.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We have also implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents.

In addition, we are offering identity protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-807-8556, going to <https://response.idx.us/BAMSI>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is August 16, 2024.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-888-807-8556 or go to <https://response.idx.us/BAMSI> for assistance or for any additional questions you may have.

BAMSI takes your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to be 'PE', written in a cursive style.

Peter Evers, President & CEO
BAMSI
10 Christy's Drive,
Brockton, MA 02301

Steps You Can Take to Protect Your Personal 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

May 16, 2024

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident that may have affected your personal or protected health information. Brockton Area Multi Services, Inc. (“BAMSI”) is committed to maintaining our clients’ trust and demonstrating our commitment to the privacy and security of all information in our possession. This letter provides information about the incident and steps you can take to protect your information.

What Happened: On April 14, 2023, BAMSI became aware of unusual activity in our network. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened. This forensic investigation determined that certain BAMSI data may have been accessed or acquired without authorization in connection with this incident. As a result, we launched a comprehensive review of the potentially affected data, then worked diligently to validate the results and confirm addresses for potentially affected individuals in preparation for notification. These efforts concluded on April 29, 2024, and identified some of your information within the potentially affected dataset.

What Information Was Involved: The potentially affected information included your <<Variable Text 1: Data Elements>>.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We have also implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents.

What You Can Do: You can follow the recommendations on the following page to help protect your information. You should also review your account statements and explanation of benefits forms and report any errors or activity you do not recognize to your insurance carrier.

For More Information: If you have any questions about this letter, please contact IDX, A ZeroFox Company at 1-888-807-8556 or go to <https://response.idx.us/BAMSI> for assistance.

BAMSI takes your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to be 'PE', written in a cursive style.

Peter Evers, President & CEO
BAMSI
10 Christy's Drive,
Brockton, MA 02301

Steps You Can Take to Protect Your Personal 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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>.

Security Freeze: You have the right to put a security freeze on your credit file at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

