LEWIS BRISBOIS BISGAARD & SMITH LLP

Donna Maddux
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Donna.Maddux@lewisbrisbois.com
Direct: 971.334.7001

May 11, 2022

VIA WEB PORTAL

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

Re: **Notification of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Behavioral Health Partners of Metro West ("BHPMW") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine data breach notification statute 10 Me. Rev. Stat. Ann. §§ 1346-1350-B.

1. Nature of the Security Incident

BHPMW operates a Behavioral Health Community Partner Program under contract with MassHealth and in collaboration with five provider agencies - Advocates, Family Continuity, SMOC, Spectrum Health Systems, and Wayside Youth and Family Support. All are located in Massachusetts.

On October 1, 2021, BHPMW discovered it was the victim of a sophisticated cybersecurity attack affecting the BHPMW network. Upon discovering this activity, BHPMW immediately took steps to secure its environment and engaged cybersecurity experts to assist with an investigation. The investigation determined that an unknown actor gained access to and obtained data from the BHPMW network without authorization between September 14, 2021, and September 18, 2021. The incident did not involve encryption, did not disrupt access to their network, and did not result in data loss. On April 5, 2022, BHPMW determined that personal information for some Maine residents may have been involved in the incident.

2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately thirteen (13) Maine residents. The information involved in the incident may differ depending on the individual but may include name, Social Security Number, date of birth, medical information, health insurance information, and other information.

The affected individuals will receive a letter notifying them of the incident, offering complimentary identity monitoring services, and providing additional steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on May 11, 2022.

3. Measures Taken to Address the Incident

After discovering the incident, BHPMW engaged industry-leading cybersecurity experts to investigate the incident. BHPMW also implemented additional security features to reduce the risk of a similar incident occurring in the future. Additionally, this incident was reported to the Federal Bureau of Investigation.

On May 11, 2022, BHPMW will notify the thirteen (13) Maine residents about this event, and advise them about steps they can take to help protect their information. In addition, BHPMW offered all impacted individuals complimentary credit monitoring and identity protection services for at least twenty-four (24) months through IDX. The identity monitoring services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

4. Contact Information

BHPMW is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me directly at 971-334-7001 or Donna.Maddux@lewisbrisbois.com.

Sincerely,

Donna Maddux

Donna Maddux of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

DM/sgg

Enclosure:
Adult Consumer Notification Letter

Behavioral Health Partners
METROWEST
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 774-2040
Or Visit:
https://response.idx.us/bhpmw
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

May 11, 2022

Re: <<Variable Text 1>>

Dear <<FIRST NAME>> <<LAST NAME>>,

Behavioral Health Partners of MetroWest ("BHPMW") is writing to inform you of a recent data security incident that may have involved your personal information. BHPMW operates a Behavioral Health Community Partner Program under contract with MassHealth and in collaboration with five provider agencies - Advocates, Family Continuity, SMOC, Spectrum Health Systems, and Wayside Youth and Family Support. Your information may have been shared with BHPMW in connection with your participation in the <<ACO>> plan. At BHPMW, we take the privacy and security of all of information in our possession very seriously. We want to notify you of the incident, provide you with steps you can take to help protect your personal information, and offer you complimentary credit monitoring and identity protection services.

What Happened? On October 1, 2021, BHPMW discovered it was the victim of a sophisticated cybersecurity attack affecting the BHPMW network. Upon discovering this activity, we took steps to secure our digital environment. We also engaged a leading cybersecurity firm to assist with an investigation to determine whether personal information may have been accessed or acquired without authorization in conjunction with the attack. The investigation revealed that an unknown actor gained access to and obtained certain data from the BHPMW network between September 14, 2021 and September 18, 2021. On April 5, 2022, we determined that some of your personal information may have been involved in this incident.

What Information Was Involved? The information that may have been impacted includes your name, Social Security Number, date of birth, medical information, health insurance information, and other information.

What Are We Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable, if possible. We are further notifying you of this event and advising you about steps you can take to help protect your information. In addition, out of an abundance of caution, we are offering you complimentary credit monitoring and identity protection services for 24 months through IDX, a national leader in identity theft protection.

IDX's services include 24 months of credit monitoring, CyberScan dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What Can You Do? Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. You can also enroll in the IDX identity protection services, which are offered to you at no cost.

To receive credit monitoring 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. You can enroll in the complimentary IDX identity protection services by calling (833) 774-2040 or going to https://response.idx.us/bhpmw and using the Enrollment Code provided above.

IDX representatives are available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Please note the deadline to enroll is August 11, 2022. Please do not discard this letter, as you will need the Enrollment Code provided above to access services.

For More Information: If you have questions or need assistance, please contact (833) 774-2040, Monday through Friday, 9:00 am to 9:00 pm Eastern Time. IDX representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

On behalf of BHPMW, thank you for your understanding about this incident. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience this matter may cause you.

Sincerely,

Anne Pelletier Parker
Executive Director, Behavioral Health Partners of MetroWest

Se você precisa desta informação em Português por favor acesse www.bhpmw.info.
如果您需要中文信息，请访问 www.bhpmw.info.
Nếu bạn cần thông tin này bằng tiếng Việt, vui lòng truy cập www.bhpmw.info.
Siw bezwen enfomasyon sa an Kreyol ale sou sit sa www.bhpmw.info.
Si necesita esta información en Español, visite www.bhpmw.info.
If you need this information in ASL, go to www.bhpmw.info.

Additional 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 2000; (202) 727-3400; oag@dc.gov

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; https://www.maine.gov/ag/.

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, https://ag.ny.gov/.

Rhode Island: <<Variable Text 3>> Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov.

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; Phone (802) 828-3171; Email: ago.info@vermont.gov.

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