

June 28, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Psych Associates of Maryland LLC d/b/a Bloom Health Centers (“Bloom Health”), a provider of mental health services based out of Maryland, 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 Maryland’s data breach notification statute.

Nature of the Security Incident

On or around November 1, 2023, Bloom Health became aware of suspicious activity within the mailbox of a user affiliated with Bloom Health. In response, Bloom Health immediately took steps to secure its environment and engaged a leading cybersecurity firm to assist with an investigation and determine whether personal or protected health information may have been accessed or acquired during the incident. As a result of the investigation, on December 6, 2023, Bloom Health identified that one (1) employee’s mailbox may have been accessed without authorization.

Bloom Health then engaged an independent team to conduct a comprehensive review of all data within the impacted mailbox, and on March 25, 2024, that review determined that the personal information of certain individuals may have been affected. Bloom Health then worked diligently to locate relevant address information to effectuate notification to such individuals, and address verification efforts were completed on June 10, 2024.

The information varied between individuals but may have included name, address, health insurance information, Medicaid / Medicare information, and medical information including details relating diagnoses, prescriptions, treatments, and procedures. Additionally, for a limited number of individuals, Social Security number, payment card number, and/or driver’s license number may have been affected. Please note that we have no current evidence to suggest misuse or attempted misuse of personal or protected health information involved in the incident.

Number of Maryland Residents Involved

On June 28, 2024, Bloom Health notified one thousand, seven hundred and fifty-three (1,753) Maryland residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, Bloom Health is providing individuals with information about steps that they can take to help protect their personal information as well as offering complimentary credit monitoring and identity protection services through IDX to individuals with certain information affected. Further, Bloom Health will be conducting a thorough review of its data security policies and procedures to identify any areas for improvement. Additionally, Bloom Health has enhanced the security of its environment and has provided additional training to all staff members on data protection best practices to minimize the risk of similar incidents in the future.

Contact Information

Bloom Health remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at LFunk@Constangy.com.

Sincerely,



Laura K. Funk
Partner
CONSTANGY, BROOKS, SMITH & PROPHETE,
LLP

Enclosure: Sample Notification Letter



Return to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

June 28, 2024

Re: Notice of Data <<Variable Text 1>>

Dear <<FirstName>> <<LastName>>,

We are writing to provide you with information about a recent data security incident experienced by Psych Associates of Maryland LLC d/b/a Bloom Health Centers (“Bloom Health”), a provider of mental health services based out of Maryland, that may have involved your personal and/or protected health information. At Bloom Health, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened. On or around November 1, 2023, Bloom Health became aware of suspicious activity in a user’s email mailbox affiliated with Bloom Health. We immediately took steps to secure the mailbox and launched an investigation with the assistance of a leading computer forensics firm to determine what happened and whether personal or protected health information may have been accessed or acquired during the incident. As a result of the investigation, on December 6, 2023, we confirmed that one employee’s mailbox may have been accessed without authorization. Bloom Health then engaged an independent review team to conduct comprehensive review of all data within the affected mailbox, which was completed on March 25, 2024. Bloom Health then worked diligently to identify up-to-date contact information for all individuals whose information was contained within the mailbox to effectuate formal notification to such individuals, and address verification efforts were completed on June 10, 2024.

What Information Was Involved. The information within the mailbox varied between individuals but may have included your <<Variable Text 2 – Data Elements>>. **Please note that we have no evidence to suggest misuse or attempted misuse of information within the affected mailbox.**

What We Are Doing. As soon as we discovered this incident, we took the steps described above. Further, we will be continuing to conduct a thorough review of our data security policies and procedures to identify any areas for improvement. Additionally, we have provided additional training to all staff members on data protection best practices to minimize the risk of similar incidents in the future.

Additionally, Bloom Health is providing you with information about steps that you can take to help protect your personal information and, as an added precaution, is offering you free of charge identity theft protection services through IDX, a ZeroFox Company. These identity protection services include: <<12/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. We recommend that you activate your complimentary IDX services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the enrollment code provided above. Representatives are available from 9:00am to 9:00pm Eastern Time from Monday to Friday. Please note that deadline to enroll is September 28, 2024. In addition, we recommend that you review the guidance included with this letter about additional steps you can take to protect your personal information.

For More Information. If you have questions or need assistance, please contact IDX at 1-800-939-4170, Monday through Friday from 9:00am to 9:00pm Eastern Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

The privacy and security of our data within our control is of utmost importance to us, and we deeply regret any concern or inconvenience this incident may cause.

Sincerely,

A handwritten signature in dark ink, appearing to read 'BVo', is positioned above the printed name and title of the sender.

Bao M. Vo, DO
Chief Quality Officer

Bloom Health Centers
1954 Greenspring Drive, Suite 530
Timonium, MD 21093

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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 proof. 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 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.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; 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; 212-416-8433; <https://ag.ny.gov/>

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

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

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



Return to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

June 28, 2024

Re: Notice of Data <<Variable Text 1>>

Dear <<FirstName>> <<LastName>>,

We are writing to provide you with information about a recent data security incident experienced by Psych Associates of Maryland LLC d/b/a Bloom Health Centers ("Bloom Health"), a provider of mental health services based out of Maryland, that may have involved your personal and/or protected health information. At Bloom Health, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident and providing you with steps you can take to help protect your personal information.

What Happened. On or around November 1, 2023, Bloom Health became aware of suspicious activity in a user's email mailbox affiliated with Bloom Health. We immediately took steps to secure the mailbox and launched an investigation with the assistance of a leading computer forensics firm to determine what happened and whether personal or protected health information may have been accessed or acquired during the incident. As a result of the investigation, on December 6, 2023, we confirmed that one employee's mailbox may have been accessed without authorization. Bloom Health then engaged an independent review team to conduct comprehensive review of all data within the affected mailbox, which was completed on March 25, 2024. Bloom Health then worked diligently to identify up-to-date contact information for all individuals whose information was contained within the mailbox to effectuate formal notification to such individuals, and address verification efforts were completed on June 10, 2024.

What Information Was Involved. The information within the mailbox varied between individuals but may have included your <<Variable Text 2 – Data Elements>>. **Please note that we have no evidence to suggest misuse or attempted misuse of information within the affected mailbox.**

What We Are Doing. As soon as we discovered this incident, we took the steps described above. Further, we will be continuing to conduct a thorough review of our data security policies and procedures to identify any areas for improvement. Additionally, we have provided additional training to all staff members on data protection best practices to minimize the risk of similar incidents in the future.

What You Can Do. We recommend that you review the guidance included with this letter about additional steps you can take to protect your personal information.

For More Information. If you have questions related to the incident, please contact IDX at 1-800-939-4170, Monday through Friday from 9:00am to 9:00pm Eastern Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

The privacy and security of our data within our control is of utmost importance to us, and we deeply regret any concern or inconvenience this incident may cause.

Sincerely,

A handwritten signature in black ink, appearing to read 'B. Vo', with a stylized flourish at the end.

Bao M. Vo, DO
Chief Quality Officer

Bloom Health Centers
1954 Greenspring Drive, Suite 530
Timonium, MD 21093

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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 proof. 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 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.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; 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; 212-416-8433; <https://ag.ny.gov/>

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

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

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