

May 2, 2024

Via E-Mail: Idtheft@oag.state.md.us

Attorney General Anthony Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Cybersecurity Incident

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Riverdale Mental Health d/b/a Mosaic Mental Health (“MOSAIC”), a mental healthcare provider based in the Bronx, New York, with respect to a cybersecurity incident that was discovered by MOSAIC on October 6, 2023 (hereinafter, the “Incident”). Please note MOSAIC takes the security and privacy of the information within its control seriously and has taken steps to prevent a similar incident from occurring in the future. This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of MOSAIC residents being notified, and the steps MOSAIC has taken in response to the Incident.

1. Nature of the Incident

On October 6, 2023, MOSAIC's anti-malware program detected and isolated unauthorized activity within its computer systems (the “Incident”). Upon being alerted of the Incident, MOSAIC engaged a specialized incident response vendor to conduct a forensic investigation to determine the extent and root cause of the incident. On November 15, 2023, the forensic investigation concluded that protected health information may have been accessed by an unauthorized user. Based upon the results of the forensic investigation, MOSAIC conducted a review of the impacted data for the purpose of notifying all those clients who were affected as a result of the Incident.

On January 3, 2024, MOSAIC determined that information impacted in the Incident likely involved individuals’ name, address, date of birth, and Social Security number. As of this writing, MOSAIC has not received any reports of related identity theft since the date of the incident (October 6, 2023, to present).

2. Number of Maryland residents affected.

MOSAIC identified two (2) Maryland residents whose information was potentially affected by this Incident. Notification letters to these individuals were mailed on April 3, 2024, by U.S. First Class mail. A sample copy of the notification letter is attached hereto under **Exhibit A**.

3. Steps taken in response to the Incident.

MOSAIC is committed to ensuring the security and privacy of all personal information within its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MOSAIC moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals.

MOSAIC is also offering complimentary credit monitoring and identity theft restoration services through Identity Force, a TransUnion company, to affected Maryland residents to help protect their identity. Additionally, MOSAIC provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

MOSAIC remains dedicated to protecting the sensitive information in its control. Should you have any questions or require additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A



[REDACTED]
[REDACTED]
[REDACTED]

April 3, 2024

VIA FIRST-CLASS MAIL

Notice of Data Security Incident

Dear [REDACTED],

Riverdale Mental Health d/b/a Mosaic Mental Health (“MOSAIC”) is writing to inform you of a recent cybersecurity incident that may have involved your protected health information. MOSAIC takes the privacy of client information very seriously and sincerely apologizes for any inconvenience this Incident may cause. This letter contains details about the Incident, steps we have taken in response to mitigate any risk, and services we are making available to protect your information.

What Happened?

On October 6, 2023, MOSAIC's anti-malware program detected and isolated unauthorized activity within its computer systems (the “Incident”). Upon being alerted of the Incident, MOSAIC engaged a specialized incident response vendor to conduct a forensic investigation to determine the extent and root cause of the incident. The forensic investigation concluded that protected health information may have been accessed by an unauthorized user. As such, MOSAIC is notifying all those clients whose information may have been impacted as a result of the Incident.

What Information Was Involved?

The investigation confirmed that client information maintained within the compromised computer systems may have been subject to unauthorized access. The data contained in this system may include protected health information such as your: [REDACTED].

While MOSAIC has no reason to believe that any client’s information has been misused, we are nonetheless notifying our clients out of an abundance of caution.

What We Are Doing

MOSAIC takes the privacy and security of our personal information very seriously, and has taken steps to prevent a similar event from occurring in the future.

In order to address any individual concerns and mitigate any exposure or risk of harm following this Incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any

questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

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].

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under eighteen (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.

What You Can Do

Although MOSAIC is not aware of any instances of misuse of any client information, we recommend that our clients take advantage of the complimentary services that are being offered. Instructions on how to enroll in these services are included in the materials enclosed with this letter. You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information on-line at www.ftc.gov/idtheft.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. MOSAIC recognizes that you may have questions not addressed in this letter. If you have additional questions, please call [REDACTED] (toll free) during the hours of 8:00 am and 8:00 pm Eastern time, Monday through Friday (excluding U.S. national holidays).

MOSAIC sincerely regrets any inconvenience or concern that this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Mosaic Mental Health

Additional Important Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 1-800-680-7289	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Identity Protection PIN: You can get a six-digit Identity Protection PIN to prevent someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. An IP PIN is used by the IRS to verify your identity when filing your electronic or paper tax return. To receive an IP Pin, you must register to validate your identity at IRS.gov. Use the Get an IP PIN tool available between mid-January through mid-November to receive your IP PIN.

<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed 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.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. 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 at www.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.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov