Jennifer S. Stegmaier
312.821.6167 (direct)
jennifer.stegmaier@wilsonelser.com

September 25, 2024

Via Email Idtheft@oag.state.md.us

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Re: Data Incident Involving Cumberland Heights Foundation

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Cumberland Heights Foundation ("Cumberland Heights"), a substance abuse rehabilitation center located at 8283 River Road, Nashville Tennessee, 37209, with respect to a recent data incident that was first discovered by Cumberland Heights on February 21, 2024 (hereinafter, the "Incident"). Cumberland Heights takes the security and privacy of the information within its control very 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 impacted, the number of Maryland residents being notified, and the steps that Cumberland Heights has taken in response to the Incident. We have also enclosed hereto a sample of the notification letter mailed to the potentially impacted individuals, which includes an offer of complimentary credit monitoring services.

1. Nature of the Incident

On February 21, 2024, Cumberland Heights detected unusual activity within its Microsoft O365 environment. Upon discovery of the Incident, Cumberland Heights immediately secured its e-mail tenant and promptly engaged a specialized third-party cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. On March 27, 2024, the forensic investigation determined that one (1) Cumberland Heights employee e-mail account may have been accessed by an unauthorized user. Cumberland Heights's e-mail environment has since been secured and remediated.

Based on the findings of the forensic investigation, Cumberland Heights engaged a third-party data mining firm to conduct a review of the information maintained within the accessed account and identify those individuals whose personal information may have been impacted by the Incident. Cumberland Heights completed its review of the accessed data on June 20, 2024, and a first wave of notification letters was mailed on August 5, 2024. Since completing the first wave of notice, Cumberland Heights has worked to identify and locate additional individuals whose information may have been impacted for purposes of providing notice and complimentary credit monitoring services to the affected individuals. Cumberland finished identifying and locating the remaining affected individuals on September 7, 2024, and a second wave of notice letters will be completed on September 26, 2024.

Based on the investigation, Cumberland Heights determined that the following types of personal information may have been impacted as a result of the Incident: names, addresses, dates of birth, drivers' license numbers, positive lab results, sensitive content, and Social Security numbers. We note the impacted data elements vary per individual. As of this writing, Cumberland Heights has not received any reports of related identity theft since the date of the incident (February 21, 2024, to present).

2. Number of Maryland residents affected.

Based on the results of the investigation and data review, Cumberland Heights identified eleven (11) Maryland residents whose information was potentially impacted as a result of the Incident. Notification letters to the individuals will be mailed on September 26, 2024, by first class mail. A sample copy of the notification letter is attached hereto as **Exhibit A.**

3. Steps taken in response to the Incident.

Cumberland Heights is committed to ensuring the security and privacy of all personal information in its control and has taken steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Cumberland Heights moved quickly to investigate and respond to the Incident, assessed the security of its systems, and is notifying the potentially affected individuals. Specifically, Cumberland Heights engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, Cumberland Heights updated systemwide password policies, updated tenant settings in Office365 that increases restrictions on user rights, updated its tenant antivirus security baseline for device and user compliance, and adopted systemwide endpoint detection and response tools.

Although Cumberland Heights is not aware of any actual or attempted misuse of the affected personal information, Cumberland Heights is offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through Cyberscout, a TransUnion company, to the affected Maryland residents to help protect their identity. Additionally, Cumberland Heights will provide guidance to individuals on how to better protect against identity theft and fraud, including 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

Cumberland Heights remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at jennifer.stegmaier@wilsonelser.com or 312-821-6167.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Jennfier S. Stegmaier

EXHIBIT A

Cumberland Heights Foundation
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

cumberland heights

[redacted]

September 26, 2024

Notice of Data Security Incident

Dear [redacted],

Cumberland Heights Foundation, Inc. ("Cumberland Heights") is writing to inform you of a recent data Incident that may have resulted in an unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the Incident, steps we are taking in response to the Incident, and resources available to help you protect against the potential misuse of your information.

What Happened?

On February 21, 2024, Cumberland Heights detected unusual activity within its e-mail environment. Upon discovery of this incident, Cumberland Heights immediately secured its environment and promptly engaged a specialized third-party cybersecurity firm to conduct a comprehensive investigation to determine the nature and scope of the incident. On March 27, 2024, the forensic investigation determined that one (1) Cumberland Heights e-mail account may have been compromised by an unauthorized actor. Cumberland Heights's e-mail environment has since been secured and remediated.

Based on these findings, Cumberland Heights conducted a review of the information maintained within the compromised accounts to identify the specific individuals and the types of information that may have been compromised. Cumberland Heights completed its initial review on June 20, 2024. Upon completion of its initial review, Cumberland Heights mailed a first wave of notice letters to the affected individuals on August 5, 2024. Since then, Cumberland Heights has worked to further identify additional individuals whose information was contained within the compromised account for purposes of providing this notice along with an offer for complimentary credit monitoring services to the affected individuals.

What Information Was Involved?

Although Cumberland Heights has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the investigation, the following information related to you may have been subject to unauthorized access: [redacted].

What We Are Doing

Data privacy and security is among Cumberland Heights's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the incident, Cumberland Heights moved quickly to investigate, respond, and confirm the security of our systems. In addition, Cumberland Heights implemented security enhancement measures to prevent a similar incident from occurring in the future, such as updating systemwide password policy, updating tenant settings in Office365 that increases restrictions on user rights, and updating its tenant antivirus security baseline for device and user compliance.

In response to the incident, Cumberland Heights is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score 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. Finally, Cumberland Heights is providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

Out of an abundance of caution, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

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. Enrolment requires an internet connection and e-mail account and may not be available to minors under the age of 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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

Should you have any questions or concerns not addressed in this letter, please call [redacted] (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

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

Sincerely,
Cumberland Heights Foundation

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TranUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

0000103O3O0000

P