NELSON MULLINS

NELSON MULLINS RILEY & SCARBOROUGH LLP
ATTORNEYS AND COUNSELORS AT LAW
Atlantic Station
201 17th Street, NW | Suite 1700
Atlanta, GA 30363
M 404.909.0665
T 404.322.6000 F 404.322.6050
nelsonmullins.com

Gina G. Greenwood, JD, CIPP/US
gina.greenwood@nelsonmullins.com

April 26, 2022

Attorney General John M. Formella
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Hon. David G. LeFrancois
State of New Hampshire
10th Circuit Court, Family Division – Brentwood
P.O. Box 1208
Kingston, NH 03848-1208

Dear Attorney General Formella and Judge LeFrancois:

We represent The Mental Health Center for Southern New Hampshire d/b/a CLM Center for Life Management ("CLM"), a non-profit community mental health organization that provides services to Participants in the Mental Health Court Diversion Program of the State of New Hampshire's 10th Circuit Court, Family Division – Brentwood. This letter is being sent to you as notice because twenty-seven (27) Participants may have been affected by a recent security incident.

Our client discovered a data security incident on February 23, 2022, and a computer consulting firm was promptly engaged to investigate the incident. The investigation team determined that an unauthorized person gained access to the computer system that CLM used to store information about individual participation in the Mental Health Court Diversion Program. The unauthorized person appears to have deleted and moved information around within the system.

However, available evidence did not reveal the removal (exfiltration) of any personal information from the system/server.

Please also note: CLM full electronic medical / treatment records were not affected, and a backup copy of the Court Diversion Program information also was not affected, so the ability to report back to the Court by CLM and the other community mental health providers was not materially affected. The investigation team also did not find any postings of personal information on the

internet or dark web and did not identify any actual misuse of personal financial or health information during the course of the investigation.

The investigation team was unable to determine whether any specific person's Court information was actually viewed. The Diversion Program information that was stored in the system varied, but the information that potentially could have been viewed could have included things such as contact information, date of birth, social security number (for twenty-two (22) of the CLM Participants), diagnosis code, medication name, and healthcare provider organizational name.

Enclosed please find the template letter(s) mailed to the twenty-seven potentially affected New Hampshire residents on April 21, 2022.

CLM's Court Liaison is attempting to reach out to each of the 27 Participants to try to ensure they are supported appropriately.

If you have questions or need additional information, please do not hesitate to contact me at (404) 322-6790 or by email at gina.greenwood@nelsonmullins.com.

Best Regards,

Gina G. Greenwood, JD, CIPP/US

Enclosure: Sample Notification Letter(s)

CLM Center for Life Management

10 Tsienneto Road
Derry, New Hampshire 03038

<NAME>
<ADDRESS>
<CITY>, <STATE> <ZIP>

April 21, 2022

Dear <NAME>:

We are notifying you of an incident that may have involved your personal information.

What happened? We discovered a data security incident on February 23, 2022, and a computer consulting firm was promptly engaged to investigate the incident. The investigation team determined that an unauthorized person gained access (on about February 21) to our computer system that we use to store information about your participation in the Mental Health Court Program. The unauthorized person appears to have deleted and moved information around within the system; however, available evidence did not reveal the removal (exfiltration) of any personal information from the system/server.

NOTE: Your CLM full medical / treatment records were ***not*** affected at all and a full backup copy of the Court Program information also was not affected, so we still have all the information we need for reporting. **This incident should not affect your participation in the Court Program in any way.**

What information was involved? The investigation team was unable to determine whether your specific court information was actually viewed. The diversion program information that was stored in our system varied, but the information that potentially could have been viewed could have included things such as your <DATA ELEMENTS>.

What are we doing in response? What you can do? The investigation team did not find any postings of personal information on the internet, and did not identify any other actual misuse of your social security number or personal information during the course of the investigation.

In an abundance of caution, we recommend you take precautions, and **we are offering you one (1) year(s) of *free* credit monitoring** and identity theft insurance through Experian - to give you peace of mind. *You must activate the free product by the activation date in order for it to be effective. The activation instructions are included with this notification.* We also have included some additional steps that you can take, as appropriate.

For more information about this incident or if you need assistance activating you ID theft monitoring, please call me at **(603) 965-0731** between the hours of 10 am to 5 pm ET Monday - Friday (excluding holidays) or you can email me at sarnault@clmnh.org.

Please do not contact the Court about this incident. Court Program officials have been notified but will not have detailed information about this event.

Feel free to contact us directly at (603) 434-1577 if you need to schedule an appointment for treatment. We sincerely apologize for any concern this may have caused you.

Sincerely,

Steve Arnault

Vice President of Clinical Services, Quality and Compliance

STEPS YOU CAN TAKE

Below is information on steps you can take to protect yourself.

➢ **ACTIVATE Your FREE Experian IdentityWorks Product NOW in Three Easy Steps.** To help protect your identity, we are offering you a **complimentary one (1) year membership** of Experian's IdentityWorks product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.

1. **ENSURE You Enroll By**: June 23, 2022 **(Your code will not work after this date.)**
2. **VISIT** the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcredit **PROVIDE Your Activation Code**: <ACTIVATION CODE>

If you have questions about the IdentityWorks or need an alternative to enrolling online, **please call 877-288-8057** and provide engagement <ENGAGEMENT NUMBER>**.** A credit card is not required for enrollment. Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Restoration Agents are immediately available to help address credit/non-credit related fraud.
- **$1 Million Identity Theft Insurance:**[2] Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the Enrollment Date (noted above) by enrolling at https://www.experianidworks.com/3bcredit or calling 877-288-8057 to register your activation code above in order for this service to be activated. Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer team at 877-288-8057.

➢ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your personal credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the

security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR ACCOUNT / CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your bank account and/or personal credit file. An initial credit file fraud alert is a 1-year alert that is placed for free on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Always carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize.

- **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it. Notification of this incident has not been delayed as a result of a law enforcement investigation.

- **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. 11) You may seek damages from violators. 12) Identity theft victims and active duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for additional information. Federal Trade Commission also provides information at www.ftc.gov/idtheft FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

CLM Center for Life Management

[No SSN]

10 Tsienneto Road
Derry, New Hampshire 03038

<NAME>
<ADDRESS>
<CITY>, <STATE> <ZIP>

April 21, 2022

Dear <NAME>:

We are notifying you of an incident that may have involved your personal information.

What happened? We discovered a data security incident on February 23, 2022, and a computer consulting firm was promptly engaged to investigate the incident. The investigation team determined that an unauthorized person gained access (on about February 21) to our computer system that we use to store information about your participation in the Mental Health Court Program. The unauthorized person appears to have deleted and moved information around within the system; however, available evidence did not reveal the removal (exfiltration) of any personal information from the system/server.

NOTE: Your CLM full medical / treatment records were ***not*** affected at all and a full backup copy of the Court Program information also was not affected, so we still have all the information we need for reporting. **This incident should not affect your participation in the Court Program in any way.**

What information was involved? The investigation team was unable to determine whether your specific court information was actually viewed. The diversion program information that was stored in our system varied, but the information that potentially could have been viewed could have included things such as your <DATA ELEMENTS>. **Your Social Security Number was not affected.**

What are we doing in response? What you can do? The investigation team did not find any postings of personal information on the internet, and did not identify any actual misuse of your social security number or other personal information during the course of the investigation.

We do not believe that this incident will cause any harm to you, but in an abundance of caution, as always, you should be on alert for phone and email scams. Never give out your Social Security or credit/debit card numbers on the phone and closely monitor financial accounts and credit reports for inaccurate information. A free copy of your credit report can be obtained annually by contacting the following: Equifax at 1-800-685-1111; Experian at 1-888-397-3742; and TransUnion at 1-800-916-8800. Report any unusual activity to law enforcement. For more information on protecting personal data, you can visit www.ftc.gov or write to FTC, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.

For more information about this incident, please call me at **(603) 965-0731** between the hours of 10 am to 5 pm ET Monday - Friday (excluding holidays) or you can email me at sarnault@clmnh.org.

Please do not contact the Court about this incident. Court Program officials have been notified but will not have detailed information about this event.

Feel free to contact us directly at (603) 434-1577 if you need to schedule an appointment for treatment. We sincerely apologize for any concern this may have caused you.

Sincerely,

Steve Arnault

Vice President of Clinical Services, Quality and Compliance