LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey, CIPP (E/US)
One PPG Place, 28th Floor
Pittsburgh, PA 15222
Lauren.Godfrey@lewisbrisbois.com
Direct: (412) 567-5113

May 4, 2022

VIA ELECTRONIC SUBMISSION

Attorney General John M. Formella
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General Formella:

We represent Community Council of Nashua d/b/a Greater Nashua Mental Health ("GNMH") in connection with a recent data security incident which is described in greater detail below. GNMH takes the privacy and security of the information within its control very seriously and is taking steps to help prevent a similar incident from occurring in the future.

1. Nature of the data security incident.

GNMH is a nonprofit entity operating as a New Hampshire Community Mental Health Center ("CMHC") providing mental health treatment services pursuant to a court diversion program funded initially in 2008 by grants awarded by the federal Bureau of Justice Assistance ("BJA"). GNMH maintains a database of records related to those services including patient name, birthdate, and potentially; address, social security number, diagnosis, medication, and program participation data within a SQL server maintained by a third-party CMHC ("Third-Party").

On February 23, 2022, Third-Party notified GNMH of a data security incident involving inappropriate access to the server that housed the database of GNMH's records, and the Third-Party had hired an external security consulting firm that was conducting a forensic investigation to determine the extent of the incident and whether there was unauthorized access to or acquisition of personal information within GNMH's Database. On April 11, 2022, Third-Party notified GNMH that the investigation determined that an unauthorized person gained access to the system. The investigation was unable to determine whether personal information within the Database was acquired. GNMH is not aware of any misuse of the information involved in the incident.

2. Number of New Hampshire residents affected.

The incident may have affected 1,067 New Hampshire residents. Notification letters were mailed to 901 affected individuals on May 4, 2022. A sample copy of the letter provided to potentially impacted individuals is included with this letter.

Additionally, a toll-free call center at (888) 994-0277 was established with and operated by Experian to answer questions about the incident, and a notice was posted on GNMH's website to provide substitute notice for the 166 New Hampshire residents who may have been affected by the incident but had an incomplete, inaccurate, or unavailable mailing address. The substitute notice may be found on GNMH's website at https://gnmhc.org.

3. Steps taken relating to the incident.

GNMH has taken significant affirmative steps to help prevent a similar situation from arising in the future and to protect the privacy and security of all sensitive information in its possession. These steps have included, but are not limited to, moving the information pertaining to the GNMH court diversion program to a new, secure location, implementing encryption and stronger password requirements, and implementing a new security risk management plan.

4. Contact information.

GNMH is committed 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 (412) 567-5113, or by e-mail at Lauren.Godfrey@lewisbrisbois.com.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey, CIPP(E/US) of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure – Template Consumer Notification Letter

GNMH Greater Nashua Mental Health

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 4, 2022

H8509-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 CREDIT MONITORING
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

We are notifying you of an incident that may have involved your personal information. Greater Nashua Mental Health ("GNMH") takes the privacy and security of your information very seriously, which is why we are informing you of the incident and offering you complimentary credit monitoring and identity protection services.

What happened? On February 23, 2022, we discovered a data security incident. In response, we immediately began an investigation with the help of cybersecurity experts. The investigation team determined that on or about February 21, 2022, an outside party gained access to the computer system that we use to store information about your participation in GNMH's mental health court diversion program. The outside party deleted and moved information around within the computer system where your information was stored. The investigation team was unable to determine whether your specific court information was actually viewed. However, the investigation did not find evidence that anyone's personal information was taken from the system. We immediately undertook a review of the information involved in the incident, and out of an abundance of caution, are notifying you to provide you with steps that you can take to protect your information.

NOTE: Your GNMH full medical / treatment records were not affected at all and a full backup copy of the court diversion program information also was *not* affected, so we still have all the information we need for reporting.

What information was involved? The diversion program information that was stored in our system varied but potentially could have included things such as your name, [Extra1].

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

Out of an abundance of caution to help protect your identity, we are offering a complimentary [Extra2]-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **July 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 994-0277** by **July 31, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your [Extra3]-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 994-0277. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for [Extra2]-year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

For more information about this incident or if you need assistance activating you ID theft monitoring, please call Experian **(888) 994-0277** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **ENGAGE#**.

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

Feel free to contact us directly at 603-889-6147 if you need to schedule an appointment for treatment. We sincerely apologize for any concern this may have caused you.

Sincerely,

Brian Huckins

Brian Huckins MS Leadership
Vice President of Quality and Corporate Compliance
Greater Nashua Mental Health
100 West Pearl Street
Nashua, NH 03060
603-889-6147 ext. 155

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant Company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 below.

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
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 Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and asks that the creditor contact you prior to establishing any accounts in your name. 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

0000001

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

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

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

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.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. You may also contact Greater Nashua Medical Center at 100 West Pearl Street, Nashua, New Hampshire 03060.