CONSTANGY
BROOKS, SMITH & PROPHETE LLP

175 Pearl Street
Suite C-402
Brooklyn, New York 11201

April 27, 2023

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident Update**

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Unlimited Care, Inc. ("UCI"), a provider of home care services, in connection with a data security incident that was previously reported to your office on April 12, 2023. We are writing to provide an update with respect to an additional New Hampshire resident that UCI notified of the incident after having completed its review of potentially impacted information relating to its patients.

1. Nature of the Security Incident

As previously reported, on February 16, 2023, UCI experienced a network disruption. In response, UCI immediately took steps to secure its digital environment and engaged a leading cybersecurity firm to assist with an investigation. Through the investigation, UCI learned that personal information may have been accessed by an unauthorized individual. On or around March 21, 2023, UCI determined that personal information of employees may have been affected. Additionally, UCI began the process of locating mailing information to effectuate notification to the employees, which was completed on March 27, 2023. UCI identified one (1) New Hampshire resident and issued notification letters to such individual on April 12, 2023.

During the investigation, UCI additionally engaged in a comprehensive review of the potentially impacted data to also identify any patients whose information may have been involved and to gather up-to-date contact information to effectuate information. UCI completed its identification efforts for these remaining individuals on April 7, 2023, after which UCI arranged for notification letters to be sent to the limited number of potentially impacted patients.

The information affected varies by individual but may have included

. Please note that we have no current evidence to suggest misuse or attempted misuse of personal information involved in the incident.

2. Number of New Hampshire Residents Involved

On April 27, 2023, UCI notified one (1) New Hampshire resident 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. Additionally, UCI posted notice of the data security incident on the home page of its website, which will remain for a period of at least ninety (90) days.

3. Steps Taken to Address the Incident

In response to the incident, UCI has taken steps to secure its network environment and implemented additional technical security measures, including but not limited to:

- Enforced a global password reset throughout the environment and confirmed completion of such on all administrative accounts;
- Deployed Carbon Black, a sophisticated endpoint detection and response tool with 24/7 monitoring on all servers, desktops, and laptops;
- Initiated geo-fencing for non-U.S. emails and shut down all non-U.S. IP address connections;
- Limited future access to the VPN to essential staff and personnel; and
- Upgraded its antivirus software.

As with UCI employees who were notified of the incident, UCI has established a toll-free call center through IDX to address questions from patients who may have been affected. Additionally, as with employees, UCI is providing patients with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering individuals complimentary credit monitoring and identity protection services through IDX.

4. Contact Information

UCI remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at .

Sincerely,

Maria Efaplomatidis,
Partner
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

Return to IDX:
<<Return Address>>

To Enroll, Please Call:
8 - 4 -
isit:
p p x s/ac t e
n o e E o en

F Na e >
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

p 2 , 0 3

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

Dear << First Name>> << Last Name>>,

e are writing to provide you with informa on about a re t d c r ty cid t ex er c lim te C e c ("UCI") that may have involved your personal information. At UCI, 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 February 16, 2023, UCI experienced a network disruption. In response, we immediately took steps to secure our digital environment and engaged a leading cybersecurity firm to assist with an investigation and determine whether sensitive or personal information may have been accessed during the incident. On or around March 21, 2023, UCI determined the personal information of limited UCI patients may have been affected. UCI then completed a comprehensive review of all affected information to identify which individuals were potentially impacted and locate relevant address information to effectuate notification to such UCI patients, which was completed on April 7, 2023. Additionally, UCI is committed to notifying all regulatory agencies as required under applicable state and federal law.

What Information Was Involved? The potentially affected information may have included your <<Variable Data 2>>. **Please note that there is no current evidence to suggest misuse or attempted misuse of the personal information.** Nonetheless, out of an abundance of caution, we are notifying you of this incident and offering resources to help you protect your personal information.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. As part of the response process, we implemented additional measures to reduce the risk of a similar incident occurring in the future. Additionally, UCI 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. These identity protection services include: <<Membership Offering Length>> of credit and CyberScan dark web 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 1-888-342-2852 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 July 27, 2023. 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 , 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.

UCI takes this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Donna McNamara, MPA, RN
Vice President and Chief Operating Officer

Unlimited Care, Inc.
707 Westchester Avenue, Suite 110
White Plains, NY 10604

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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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).

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 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 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 requests 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.

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.

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.

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

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

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.