LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

File No. 28759.1574

December 7, 2022

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 0330
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Formella:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Blakehurst, a senior living community based out of Towson, Maryland, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

1. Nature of the Security Incident

On or around February 7, 2022, Blakehurst became aware of suspicious activity in its email environment. Blakehurst then launched an internal investigation and engaged an independent computer forensics firm to determine the scope of the incident and whether personal information was impacted. In March 2022, it was determined that employee email accounts may have been accessed without authorization. Blakehurst then engaged an independent vendor to perform a comprehensive review of the information that could have potentially been accessed in connection with the incident.

On August 5, 2022, Blakehurst determined that information related to certain individuals, including the personal information of New Hampshire residents, was potentially impacted. Blakehurst then worked diligently to obtain contact information to notify all affected individuals, and this process was completed on September 20, 2022. These individuals were notified through U.S. First-Class Mail on December 6, 2022. Additionally, Blakehurst 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.

The impacted information varies for each person but may have included the full name, address, date of birth, driver's license number, Social Security number, financial account number with access method, health insurance information, and/or health information. To date, Blakehurst has no evidence that any potentially impacted information has been misused in conjunction with this incident.

2. Number of New Hampshire Residents Affected

Blakehurst notified two (2) New Hampshire residents of this data security incident via U.S. First-Class Mail on December 6, 2022. A sample copy of the notification letter sent to the affected individuals is included in this letter.

3. Steps Taken Relating to the Incident

Blakehurst has implemented additional security measures to secure its email environment and reduce the risk of a similar incident occurring in the future and to protect the privacy and security of all personal information in its possession. In addition, Blakehurst is offering complimentary credit and identity monitoring services through Experian to the notified individuals. Blakehurst has also established a toll-free call center through Epiq to answer any questions about the incident and address related concerns. The call center is available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

4. Contact Information

Blakehurst 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 214.722.7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Very truly yours,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN/rlw
Encl: Sample Consumer Notification Letter

BLAKEHURST

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: <<Variable Header>>

Dear <<Name 1>>,

We are writing to provide you with information about a recent data security incident experienced by Chestnut Partnership d/b/a Blakehurst ("Blakehurst"), a senior living community based out of Towson, Maryland, that may have involved your personal information. The purpose of this letter is to notify you about this incident, offer complimentary identity monitoring services, and inform you about steps you can take to help safeguard your personal information.

What Happened. On or around February 7, 2022, Blakehurst became aware of unusual activity in its email environment. In response, we immediately took steps to secure our digital environment and engaged a leading cybersecurity firm to assist with an investigation. This investigation determined that some employee email accounts may have been accessed without authorization. We then engaged a vendor to complete a comprehensive review of the potentially affected data and on August 4, 2022, determined that some individuals' personal information may have been involved in this incident. We then worked diligently to obtain contact information for impacted individuals in order to send notification. This process was concluded on September 20, 2022.

Please note this incident was limited to select information transmitted by email. There is no evidence to suggest an impact to Blakehurst's internal digital environment. Additionally, Blakehurst is not aware of any misuse or attempted misuse of information.

What Information Was Involved. The potentially affected information may have included your <<Breached Elements>>.

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 measures to enhance the security of our email environment to reduce the risk of a similar incident occurring in the future.

Additionally, Blakehurst 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 complimentary identity theft protection services through Experian. These identity protection services include: <<CM Length>> months of Experian's® IdentityWorks, which includes credit monitoring and identity restoration services, an Experian credit report, and up to a $1,000,000 identity theft insurance policy. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: <<Enrollment Deadline>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: <<Activation Code>> and reference engagement number <<Engagement Number>>
- If you need assistance with enrolling in the identity protection services, please contact (877) 288-8057.

What You Can Do. We recommend that you follow the instructions included with this letter to help protect your personal information. Blakehurst also encourages you to enroll in the complimentary services being offered to you through Experian by using the enrollment code provided.

For More Information. Further information about how to protect your personal information is included with this letter. If you have questions about this incident, please call our dedicated assistance line at 888-557-5310, Monday through Friday from 9:00 a.m. to 9:00 p m. Eastern Time, excluding major U.S. holidays.

Blakehurst 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,

Marc Strohschein
Executive Director

Blakehurst
1055 W. Joppa Road
Towson, MD 21204

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 incidents 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 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 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.