September 30, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Portal: https://appengine.egov.com/apps/me/maine/ag/reportingform

Attorney General Aaron Frey
Office of the Attorney General
Attn: Security Breach Notification
Department of Professional & Financial Regulation
Bureau of Consumer Credit Protection
35 State House Station
Augusta, Maine 04333

Re: Cybersecurity Incident Involving Keswick Multi-Care Center

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Keswick Multi-Care Center ("Keswick"), a health care organization operating a nursing home in Baltimore, Maryland, with respect to a recent data privacy incident that was first discovered by Keswick on May 9, 2022 (hereinafter, the "Incident"). Keswick takes the security and privacy of the information in 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 compromised, the number of residents being notified, and the steps Keswick has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On May 9, 2022, Keswick was subject to a data security incident that impacted its email environment. On May 26, 2022, Keswick became aware of a potential compromise of personal data when it was discovered that a file containing sensitive information may have been accessed by an unauthorized party in a compromised email account. Immediately after discovering the file, Keswick engaged with third party cybersecurity experts to determine the nature and scope of the incident. The investigation, which concluded on July 7, 2022, revealed that an unauthorized party gained access to a compromised email account and may have viewed personal data stored on that account. Then, in July and August, 2022, Keswick worked to identify the specific individuals impacted by the underlying incident in order to provide sufficient notice. Keswick was unable to identify any specific individuals impacted and has no reason to believe that any individual's information has been misused as a result of this event. Therefore, out of an abundance of caution, Keswick notified all of its residents, regardless of whether their information was in fact subject to unauthorized access.

Although Keswick is unaware of any fraudulent misuse of information, it is possible that individual's name, date of birth, Social Security number, and Medical Assistance number may have been exposed as a result of this unauthorized activity.

As of this writing, Keswick has not received any reports of related identity theft since the data of the Incident (May 9, 2022 to present).

2. Number of Maine residents affected.

A total of one (1) Maine resident may have been potentially affected by this incident. A notification letter to this individual was mailed on September 30, 2022, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Keswick is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Keswick moved quickly to investigate and respond to the Incident. Additionally, Keswick took mitigating steps which includes: restricted remote access to only authorized individuals, implemented multi-factor authentication for remote access where possible, implemented best practices to email and file environments, put more rigorous auditing process in place for Keswick's systems, and performed internal/external penetration testing and vulnerability scans.

Although Keswick is not aware of any actual or attempted misuse of the affected personal information, Keswick offered twenty-four (24) months of complimentary credit and dark web monitoring and identity theft restoration services through CyberScout to individuals to help protect their identity. Additionally, Keswick provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for 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

Keswick Multi-Care Center 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 Anjali.Das@wilsonelser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

Keswick Multi-Care Center, Inc.
P.O. Box 3923
Syracuse, NY 13220

KESWICK

[redacted]

September 30, 2022

Notice of Data Security Incident

Dear [redacted]

We are writing to inform you of a data security incident which affected Keswick Multi-Care Center ("Keswick"), a nursing home located in Baltimore, Maryland. This may have compromised personal data of some residents. This letter contains information about the incident and about how to protect your personal data, as a precaution, even though we have no indication that your information has been misused. Please accept our apologies for any inconvenience this may cause. We are notifying you out of an abundance of caution and transparency.

What Happened

On May 9, 2022, Keswick was subject to a data security incident that impacted its email environment. On May 26, 2022, Keswick became aware of a potential compromise of personal data when it was discovered that a file containing sensitive information may have been accessed by an unauthorized party. Immediately after discovering the file, Keswick engaged with third party cybersecurity experts to determine the nature and scope of the incident. The investigation, which concluded on July 7, 2022, revealed that an unauthorized party gained access to a compromised email account and may have viewed personal data stored on that account. Then, in July and August 2022, Keswick worked to identify the specific individuals impacted by the underlying incident in order to provide sufficient notice. Keswick was unable to identify any specific individuals impacted and has no reason to believe that any individual's information has been misused as a result of this event. **Therefore, out of an abundance of caution, Keswick is providing notice to all Keswick residents from the relevant time period, regardless of whether their information was in fact subject to unauthorized access.**

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you as a precaution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to: [redacted]. **However, please note that the information did not include any individual's financial account information, debit or credit card numbers.**

What We Are Doing

The security and privacy of resident information contained within Keswick's systems is a top priority, and Keswick is taking additional measures to protect this information. Since the incident, Keswick has continued to strengthen its security posture by adding the following security controls: Restricted remote access to only authorized individuals, implemented multi-factor authentication for remote access where possible, implemented best practices to email and file environments, put more rigorous auditing process in place for our systems, and performed internal/external penetration testing and vulnerability scans.

In response to the incident, we are providing you with access to the following services:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are 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, we are 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 through Identity Force, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to **https://secure.identityforce.com/benefit/keswick** 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 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 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.

What You Can Do

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 *Additional Important Information*, to learn more about how to protect against the possibility of information misuse.

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call 1-800-405-6108 between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays.

Sincerely,

Office of the Keswick Privacy & Security Officer

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is

intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
(800)-525-6285	(888)-397-3742	(800)-680-7289
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.