POLSINELLI

1401 Eye Street NW, Suite 800, Washington, DC 20005 • (202) 783-3300

December 30, 2021

Iliana L. Peters
202.626.8327
202.783.3535 Fax
ipeters@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent A New Leaf, Inc. ("A New Leaf"), 868 University DR., Mesa, Arizona 85203, in connection with a recent incident that may have affected the personal information of two (2) New Hampshire residents and are reporting a potential data security incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While A New Leaf is notifying you of this incident, A New Leaf does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

A New Leaf is a non-profit organization that assists families in need with shelter, housing, health care, and financial assistance. On March 30, 2021, A New Leaf discovered that its system was affected by a ransomware event that encrypted certain files. Upon learning of the situation, it promptly began an investigation with the help of a leading cybersecurity firm. In the course of the forensic investigation, A New Leaf learned that an unauthorized third party had gained access to certain files on its network, which may have contained personal information. A New Leaf is providing notice to anyone whose personal information could have been acquired. The information at issue for the New Hampshire residents include names and Social Security numbers.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On October 11, 2021, A New Leaf determined that the incident potentially impacted two (2) New Hampshire residents. A New Leaf is mailing the notification letter to the individuals via USPS mail on December 30, 2021 and is providing twelve (12) months of complimentary credit

monitoring and identity theft protection services. Enclosed is a copy of the notice that A New Leaf is sending to the impacted individuals.

STEPS TAKEN RELATING TO THE INCIDENT

Upon becoming aware of the incident, A New Leaf promptly launched an internal investigation and took steps to secure its systems. A New Leaf also engaged a third-party forensic security firm through legal counsel to investigate the incident and confirm the security of its computer systems. A New Leaf has also implemented additional controls to reduce the risk of a similar incident, including the adoption of endpoint monitoring. Finally, as discussed above, A New Leaf conducted a comprehensive review to determine if any personal information was involved and notified individuals accordingly.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Iliana L. Peters

Enclosure

A New Leaf, Inc.
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

A-17141

[redacted] Apt 202
[redacted]

December 30, 2021

RE: NOTICE OF DATA BREACH

Dear [redacted]

A New Leaf, Inc. ("A New Leaf") values and respects the privacy of the members of its community and the confidentiality of your information entrusted to us. Unfortunately, we are writing to advise you of a recent incident that may have impacted some of your personal information. **Although we are not aware of any instances of fraud or identity theft that have occurred as a result of this incident**, we felt that we should notify you and provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On March 30, 2021, we discovered that our system was impacted by a ransomware event that encrypted certain files. Upon learning of the situation, we promptly began an investigation with the help of a leading cybersecurity firm. This investigation was focused on identifying how the incident happened, confirming that the incident was contained, and identifying potential steps the organization could take to reduce the risk of a similar incident in the future. In the course of our investigation, we learned that certain files were copied from our system in connection with the attack. Upon identifying this, we began a review of those files to determine what, if any personal information may have been impacted.

What Information Was Involved? Based on the nature of the incident and the systems it impacted, we believed that the incident did not involve any protected health information. Based on the investigation however, on June 23, 2021, we discovered that some of the impacted documents may have contained protected health information, or other personal information, not health related. However, it was not until October 11, 2021, after a manual review of all the documents, that we were able to determine who was potentially impacted by the incident and where they resided.

What We Are Doing. As noted above, upon identifying the incident we began an investigation and took steps to ensure the that our network was secure. Additionally, based on that investigation, we are notifying you of the incident and providing you with information on steps you can take to protect yourself against identity theft and other types of fraud. Finally, although we are not aware of any instances of fraud or identity theft, we are offering a complimentary one-year membership of Experian IdentityWorks^{SM} Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important* Information sheet. We also encourage you to activate the credit monitoring services we are providing to you.

Other Important Information. We take our responsibility to safeguard personal information seriously and we appreciate your cooperation as we worked to resolve this incident. For further information and assistance, please call 1-800-872-4923, Monday through Friday from 7:00 am to 4:00 pm MT.

Sincerely,

A New Leaf, Inc.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: [redacted]

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 877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists 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.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. 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 care team at 877-288-8057.

* 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.

ADDITIONAL IMPORTANT INFORMATION

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing account statements and monitoring 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.

The Federal Trade Commission (FTC) is a good resource and you may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. The FTC can be reached at www.ftc.gov/idtheft or by calling 1-877-ID-THEFT (1-877-438-4338). You may also mail them at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by 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 can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting agencies as follows:

Equifax	Experian	TransUnion
1-800-349-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

California Residents: This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: 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.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Washington, DC Residents: Washington, DC residents can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.