Holland & Knight

811 Main Street, Suite 2500 | Houston, TX 77002 | T 713.821.7000 | F 713.821.7001
Holland & Knight LLP | www.hklaw.com

April 20, 2023

Via E-Mail DOJ-CPB@doj.nh.gov

NH Department of Justice
John M. Formella, Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of data security incident

To the Department of Justice:

I am writing on behalf of Sempermed USA, Inc. ("Sempermed") to notify your office of an incident that involves the personal information of approximately three (3) New Hampshire residents.

On or about March 2, 2023, Sempermed suffered a ransomware incident. Sempermed immediately took measures to protect its systems and to begin restoring its affected systems and data.

Sempermed also engaged a reputable third-party forensic consulting team to investigate the incident. The investigation revealed the criminal actor had apparently taken data from two of Sempermed's servers in Florida in connection with the ransomware attack. The investigation could not determine what specific data was taken, but some of Sempermed's human resources files and vendor records were potentially included in the incident. Sempermed undertook a careful review of the potentially affected records in order to make an appropriate notification to affected individuals.

Sempermed's review revealed such records included the following: for employees:

The notification letters sent to the affected individuals specify which type(s) of personal information were potentially involved.

Sempermed has arranged for IDX to provide identity protection services for the affected individuals, including complimentary credit monitoring for twenty-four (24) months.

As part of an ongoing commitment to information security, Sempermed has enhanced its security and continues to evaluate additional measures to protect against this type of incident in the future.

Notification letters are being sent today to affected individuals by U.S. mail. A sample notification letter is enclosed.

Respectfully,

Bart Huffman

cc: Franz-Michael Hohensinn, Sempermed

Enclosure: Employee Notification Letter

Sempermed USA, Inc.
Return Mail to IDX
4145 SW Watson Ave, Suite 400
Beaverton, OR 97005

sempermed®
A MEMBER OF THE SEMPERIT-GROUP

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 20, 2023

Re: Notice of Data Security Incident

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

Sempermed USA, Inc. ("Sempermed") respects your privacy, and we are writing to let you know about a cybersecurity incident that potentially involves your personal information.

What Happened

Sempermed learned on or about March 2, 2023 that it was the victim of a ransomware attack. Sempermed immediately took measures to protect its systems and to begin restoring the affected systems and data. A reputable third-party forensic consulting team was engaged, and an investigation was commenced. The investigation revealed that, in connection with the ransomware attack, the criminal actor had apparently taken data from two of Sempermed's servers in Florida. The investigation could not determine what specific data was taken, but it is possible your personal information was included.

What Personal Information Was Involved

Some of Sempermed's human resources files were potentially included in the incident. These records include .<<Variable Data 2>>

What We Are Doing

Sempermed has undertaken a careful review of the potentially affected records in order to make an appropriate notification to affected individuals. In addition, we continue to search for any misuse of information from the affected servers. To date, we have not discovered any public disclosure or other misuse of such information after the incident, on the "dark web" or otherwise.

As an added precaution, we have arranged for IDX, a ZeroFox Company, to protect your identity and help you recover from potential identity theft, at no cost to you. Part of this benefit is automatic and there is no need for you to enroll. This automatic benefit consist of fully managed identity theft recovery services. If you have an identity theft issue, simply call IDX at 1-800-939-4170 for assistance. Other services require that you actively enroll with IDX (again, at no cost to you). These optional services are described in more detail below. You must enroll by July 20, 2023 to obtain these optional services.

What You Can Do

You should read the enclosed "Information About Identity Theft Protection."

We also encourage you to take advantage of the identity recovery and protection services that we have engaged IDX to provide at no cost to you for 24 months.

As stated above, you are automatically covered for the fully managed identity theft recovery services, so there is no need to enroll for this benefit. If you have an identity theft issue, simply call IDX at 1-800-939-4170 for immediate assistance.

You must, however, enroll if you wish to take advantage of IDX-provided credit monitoring and Cyberscan monitoring assistance, and a $1,000,000 insurance reimbursement policy. These services, which are further described in the enclosed "Additional Product Information from IDX," are provided as a complimentary 24-month membership. To enroll and start monitoring your personal information and obtain insurance coverage, please follow the steps below:

- Visit the IDX website to enroll: https://app.idx.us/account-creation/protect.
- Call IDX to enroll: 1-800-939-4170. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.
- Enroll by your enrollment deadline, which is July 20, 2023.

In addition, please be on the lookout for any scams that attempt to lure you into providing personal information in connection with this incident. We will not call you or send you any email messages asking for your personal information or credit card information, or send you any email messages asking you to "click" on any links to activate credit monitoring. You should not provide information in response to any such calls or email messages, and you should not click on any links within any such email messages. The only way for you to contact IDX and/or to set up the identity protection and credit monitoring services we have obtained for you is as set forth in this letter.

For More Information

For additional information and assistance, please call .

***

Sempermed sincerely apologizes for any inconvenience that this incident may have caused. We are committed to protecting your personal information, and we will continue to review and update our protective systems and processes during this time of pervasive and ever-evolving cybersecurity threats.

Sincerely,

Doug Anderson

President, Sempermed USA, Inc.

<<Variable Data 3>>

(Enclosure)

Information About Identity Theft Protection

Remain Vigilant. We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. Purchase a copy of your credit report from the national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, GA 30374, 1-866-349-5191, www.equifax.com

Experian: P.O. Box 2002, Allen, TX 75013, 1-866-200-6020, www.experian.com

TransUnion: P.O. Box 1000, Chester, PA 19016, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you do not recognize. Look for inaccurate information, such as home address or Social Security number. If you see anything you do not understand or that looks incorrect, call the credit reporting agency at the telephone number on the report.

We recommend you vigilantly review your account statements and credit reports and promptly report any suspicious activity or suspected identity theft to law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or your state's regulatory authority to obtain information about avoiding identity theft. Contact the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Law Enforcement. Please note that law enforcement has not requested that we delay sending this notification.

State-specific Requirements.

For Maryland residents: You may obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, https://www.marylandattorneygeneral.gov/.

For New York residents: You may obtain information regarding security breach response and identity theft prevention and protection from the New York Department of State, Division of Consumer Protection, 1-800-697-1220, https://www.dos.ny.gov/consumerprotection/identity_theft/.

For North Carolina residents: You may obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1-877-5-NO-SCAM (66-7226), https://ncdoj.gov.

For Oregon residents: You may obtain information regarding identity theft prevention and report suspected identity theft to the Oregon Department of Justice, https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/, 877-877-9392.

For Rhode Island residents: You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, 150 South Main Street, RI 02903, 401-274-4400, http://www.riag.ri.gov/. As per Rhode Island law, notice is hereby given that we believe one Rhode Island resident was affected by this incident.

Fraud Alerts: You can place two types of fraud alerts on your credit report to notify creditors: an initial alert and an extended alert. You may place an initial fraud alert on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert lasts for one year. You may place an extended alert on your credit report by mail if you have been a victim of identity theft with the appropriate documentary proof. An extended fraud alert lasts for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number or visiting the website of any of the three national credit reporting agencies listed below. You only need to notify one agency, because it must notify the other two agencies.

Equifax: 1-866-349-5191, https://www.equifax.com/personal/education/identity-theft/fraud-alert-security-freeze-credit-lock/

Experian: 1-888-397-3742, https://www.experian.com/fraud/center.html

TransUnion: 1-800-680-7289, https://www.transunion.com/fraud-alerts

Credit Freezes: You may put 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 and/or password that may be issued to you when you initiate a 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 access your credit report unless you lift the freeze.

Therefore, using a credit freeze may delay your ability to obtain credit. There is no fee to place, lift and/or remove a credit freeze. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency*. Contact the three major credit reporting agencies to place a credit freeze and learn more information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 https://www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 https://www.transunion.com/credit-freeze

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

IDX
A ZEROFOX COMPANY

Additional Product Information from IDX

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.