EXHIBIT 1

We represent NuLife Med, LLC ("NuLife") located at 250 N. Commercial Street, Suite 3003, Manchester, NH 03101, and are writing to notify your office of an incident that may affect the security of certain personal information relating to twenty five (25) Maine residents. By providing this notice, NuLife does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 11, 2022, NuLife became aware of suspicious activity relating to their systems. NuLife immediately launched an investigation, aided by third-party forensic specialists, to determine the full nature and scope of the activity and to restore functionality to impacted systems. The investigation determined that certain information stored within NuLife's environment was potentially viewed or taken by an unauthorized actor, and that this activity likely occurred between March 9, 2022 and March 11, 2022. Other than a limited number of files, NuLife could not say with certainty what files were potentially viewed or taken by the unauthorized actor. However, the investigation confirmed that data potentially containing sensitive personal information related to individuals was within a network drive from which data was taken. Because NuLife could not determine that there was a low probability of compromise to this data, NuLife provided notice to all current and former patients and potential patients that were in NuLife's systems. NuLife also posted notification on their website and provided notification to prominent media where required under HIPAA.

NuLife also conducted a review of the data that was potentially impacted, with the assistance of third-party subject matter specialists. That review was recently completed.

The information that could have been subject to unauthorized access includes name, address, Social Security number, financial account information, and medical and/or health insurance information.

Notice to Maine Residents

On or about December 19, 2022, NuLife provided written notice of this incident to twenty five (25) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, NuLife moved quickly to investigate and respond to the incident, assess the security of NuLife systems, and identify potentially affected individuals. Further, NuLife notified federal law enforcement regarding the event. NuLife is also working to implement additional safeguards and training to its employees. NuLife is providing and/or previously provided access to credit monitoring services for 12 months through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, NuLife is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of

identity theft or fraud to their credit card company and/or bank. NuLife is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, contact details for the 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

NuLife is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. NuLife is also notifying the U.S. Department of Health and Human Services and notified prominent media where required pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

Return Mail Processing Center
PO 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>>

NOTICE OF <<VAR DATA 2 – HEADER>>

Dear <<Name 1>>,

NuLife Med, LLC ("NuLife") is writing to provide you with notice of a recent data privacy event that may have impacted the security of some of your information. Although at this time there is no indication that your information has been used to commit identity theft or fraud in relation to this event, we are providing you with information about the event, our response to it, and information related to what you may do to better protect your information against threats from any source, should you feel it appropriate to do so.

Who is NuLife Med, LLC? NuLife is a medical equipment company that primarily provides cold, compression and clot prevention therapy for individuals who have had orthopedic and podiatric surgeries in the United States.

What Happened? On or about March 11, 2022, NuLife became aware of suspicious activity relating to its systems. NuLife immediately launched an investigation to determine the full nature and scope of the activity and to restore functionality to impacted systems. The investigation determined that certain information stored within our environment was potentially viewed or taken by an unauthorized actor between March 9, 2022 and March 11, 2022. Other than a limited number of files, we cannot say with certainty what files were viewed or taken by the unauthorized actor. We therefore conducted a comprehensive and time-intensive review of potentially impacted files, in an abundance of caution. We recently completed that review, and determined that some of your information was found in the potentially impacted files.

What Information Was Involved? Our investigation determined that at the time of the event, your <<Breached Elements>> were present within the potentially impacted files. To date, NuLife has not received any reports of fraudulent misuse of any information potentially impacted by this event.

What We Are Doing. We take this event and the security of your information seriously. Upon learning of this event, we moved quickly to investigate and respond to the event, assess the security of our systems, and identify any impacted data. We also notified federal law enforcement about this event.

While we have no indication at this time of any identity theft or fraud has resulted from this event, as an added precaution, we are offering you access to complimentary credit monitoring services for 12 months through TransUnion. If you wish to activate the credit monitoring services, you may follow the instructions included in the *Steps You Can Take to Protect Your Personal Information*.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Your Personal Information* which contains information on what you can do to better safeguard against possible misuse of your information. You can also enroll to receive the complimentary credit monitoring and identity protection services through TransUnion. We also 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 activity.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-855-939-3980. This toll-free line is available Monday-Friday 9:00am EST – 9:00pm EST.

We sincerely regret any inconvenience this event may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Neil F. Costello
President
NuLife Med, LLC

Steps You Can Take to Protect Your Personal Information

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code <<Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. NuLife Med, LLC is located at 250 N. Commercial Street, Suite 3003, Manchester, NH 03101.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI #>> Rhode Island residents impacted by this incident.