Morgan Lewis

December 8, 2023

VIA US MAIL

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Notice of Data Security Incident of Progress Software as Vendor to Independent Living Systems, LLC*

Dear Office of the Attorney General:

This Firm represents Independent Living Systems, LLC ("ILS"), located at 4601 N.W. 77th Avenue, Miami, Florida 33166. ILS is writing to notify your Office of a recent data security incident involving the secure file transfer software tool MOVEit Transfer provided by a third-partly vendor, Progress Software. As a result of this incident, ILS and Florida Community Care, LLC are notifying 1 resident of New Hampshire.

Like many organizations, ILS used MOVEit Transfer to transfer files. As your office is likely aware, Progress Software announced a previously unknown critical zero-day vulnerability in MOVEit Transfer and recommended users disable the software until it could be patched due to a potential risk of data exposure. ILS immediately ceased using MOVEit Transfer and disabled it in its system. ILS transitioned to other solutions and never resumed use of MOVEit, but out of an abundance of caution ILS deployed all patches for MOVEit from Progress immediately upon their release. Immediately upon the Progress Software announcement, ILS launched an investigation with the assistance of cyber experts to determine whether the vulnerability had been exploited in ILS' environment and the extent of any such exploitation. ILS also notified law enforcement. On October 27, 2023, the investigation revealed that an unauthorized third party may have taken certain information that was transferred through MOVEit Transfer that may have contained personal information and protected health information related to 1 New Hampshire resident, with information including

.

Although there is no indication that the disclosed personal information has been used for any fraudulent purpose, ILS, through TransUnion, is providing written notice of the incident to individuals identified as potentially affected, both as a direct provider of services and on behalf of certain data owner clients. The notice letter explains what happened, what information was involved, what ILS has done, and how affected individuals can contact TransUnion with questions surrounding the incident. A copy of the notice letter is attached hereto as Exhibit A. ILS is also offering

Morgan, Lewis & Bockius LLP

2222 Market Street
Philadelphia, PA 19103-2921
United States

T +1.215.963.5000
F +1.215.963.5001

of credit monitoring to affected individuals and providing notice to the three major consumer reporting agencies (i.e., Equifax, Experian, and TransUnion).

ILS carefully evaluates the cybersecurity posture of third-party file transfer tools, and ILS will continue this effort. ILS is also taking steps to further secure its use of all third-party transfer tools.

Should you have any questions regarding this notification or any other aspects of the data security incident, please feel free to contact me.

Regards,

Gregory T. Parks

Enclosure

EXHIBIT A

Independent Living Systems, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

INDEPENDENT Living Systems

December 8, 2023

Re: Notice of Data Security Incident

Dear :

Independent Living Systems, LLC ("ILS" or "we") provides services to several health plans and their members. We take very seriously the protection of the information entrusted to us in providing services.

We are writing to let you know about an event that may have involved your personal information and/or protected health information. It is important to note that we have no evidence at this time that your information has been used in a wrong way, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation. Please read this letter carefully, because it provides details about what happened and what we are doing about it.

What Happened?

Like many companies, we use third party file transfer tools to move data. One such tool that is trusted by over 2,000 companies is MOVEit Transfer, a product offered by Progress Software. On May 31, 2023, Progress reported a previously unknown security vulnerability in MOVEit Transfer. ILS quickly ceased using MOVEit Transfer, disabled it in our system, and have not resumed its use. We have moved to other solutions for transfers and have not used MOVEit since the announcement of the vulnerability. Upon learning of the MOVEit Transfer vulnerability, we immediately launched an investigation to understand the potential impact.

What Information Was Involved?

Based on our investigation, it is possible that personal information including your personal health information or PHI were affected, including potentially your . While there is no evidence that the information has been used in a wrong manner, we did want to make you aware of the situation to be careful and so you can take the steps outlined below to protect yourself.

What We Are Doing

Immediately upon learning of this incident, we launched an investigation with the assistance of cyber experts, law enforcement, and outside lawyers. Please be assured that when we select third parties who provide us tools like this, we carefully evaluate the security features of the tool. We will continue this effort.

INDEPENDENT *Living Systems*

To help protect your identity, we are providing you with access to credit monitoring and remediation services at no charge through Cyberscout's Identity Force, a TransUnion company specializing in fraud assistance and remediation services. These services provide you with alerts for two years 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 to your credit file takes place with the bureau. These services also provide you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/independentliving** and follow the instructions provided. When prompted please provide the following unique code to receive services: . 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

To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and to block that credit from being established if you were not the one who initiated it.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.
- Representatives from TransUnion 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 1-833-960-4740 and supply the fraud specialist with your unique code listed above.

For More Information

If you have questions or concerns or learn of any suspicious activity that you believe may be related to this incident, please call . Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,

Stuart F. Williams
General Counsel & Chief Compliance Officer
Independent Living Systems, LLC

INDEPENDENT Living Systems

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

INDEPENDENT *Living Systems*

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov

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

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

INDEPENDENT *Living Systems*

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with 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. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.