



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 14, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Independent Living Systems, LLC (“ILS”) located at 4601 N.W. 77th Avenue, Miami, FL 33166. ILS is writing to notify your Office of an incident that may affect the privacy of certain personal information relating to approximately two thousand five hundred seventy-seven (2,577) Maryland residents. As a result of this event, ILS is issuing notification to impacted individuals as a direct provider of services and on behalf of certain data owner clients. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ILS does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 5, 2022, ILS experienced an incident involving the inaccessibility of certain computer systems on its network. ILS responded to the incident immediately and began an investigation with the assistance of outside cybersecurity specialists. Through its response efforts, ILS learned that an unauthorized actor obtained access to certain ILS systems between June 30 and July 5, 2022. During that period, some information stored on the ILS network was acquired by the unauthorized actor, and other information was accessible and potentially viewed.

Upon containing the incident and reconnecting its computer systems, ILS conducted a comprehensive review to understand the scope of potentially affected information and identify the individuals to whom such information relates. ILS received the results of this review on January

17, 2023, and then worked as quickly as possible to validate the results and provide notice to potentially impacted individuals and entities. This process included efforts to locate/validate address information for the individuals identified and confirm whether the potentially impacted individuals are affiliated with data owner clients other than ILS. Once complete, ILS moved as quickly as possible to mail letters to potentially affected individuals, provide notice to state and federal regulators, as required, and provide notice to the three major consumer reporting agencies (*i.e.*, Equifax, Experian, and TransUnion).

The personal information related to Maryland residents that could have been subject to unauthorized access includes name, Social Security number, financial account information, taxpayer identification number, medical information, health insurance information, and full access credentials to an online account.

Notice to Maryland Residents

While its review efforts were ongoing, ILS provided notice to potentially affected individuals on September 2, 2022 by posting preliminary notice of this data event on its website. Now that its review and validation efforts are complete, on March 14, 2023, ILS began providing written notice of this event to individuals identified as potentially affected, both as a direct provider of services and on behalf of certain data owner clients, including approximately two thousand five hundred seventy-seven (2,577) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notification is also being provided pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”). A list of data owner clients on whose behalf ILS provided notification will be supplied upon request.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, ILS moved quickly to investigate and respond to the incident, assess the security of ILS systems, and identify potentially affected individuals. Further, ILS notified federal law enforcement regarding the event. ILS is also working to implement additional safeguards and training to its employees. ILS is providing access to credit monitoring services through Experian, to certain individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, ILS 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 the associated institutions. ILS is providing individuals with information on how to place a fraud alert and credit freeze on one’s credit file, the 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.

ILS 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. ILS is also

Office of the Attorney General

March 14, 2023

Page 3

notifying the U.S. Department of Health and Human Services and prominent media pursuant to HIPAA.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/aml
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

12 1 3002 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



March 14, 2023

NOTICE OF DATA [EXTRA6]

Dear Sample A. Sample:

Independent Living Systems, LLC (“ILS” or “We”) provides a variety of managed services to several partner health plans and their enrollees or referred individuals, including [Extra4]. ILS’s services include plan administration, nutrition support, and comprehensive care management. We are committed to protecting the confidentiality and security of the information we gather in providing these services.

We are writing to make you aware of a data incident that may impact the privacy of your personal information and/or protected health information (“PHI”). Please read this letter carefully, as it provides details about the incident and our response.

What Happened? On July 5, 2022, we experienced an incident involving the inaccessibility of certain computer systems on our network. We responded to the incident immediately and began an investigation with the assistance of outside cybersecurity specialists. Through our response efforts, we learned that an unauthorized actor obtained access to certain ILS systems between June 30 and July 5, 2022. During that period, some information stored on the ILS network was acquired by the unauthorized actor, and other information was accessible and potentially viewed. Upon containing the incident and reconnecting our computer systems, we began to review the potentially affected data to determine whether it contained any personal information or PHI, and if so, to whom such information related.

What Information Was Involved? As previewed above, we conducted a comprehensive data review exercise to understand the scope of potentially affected information and identify the individuals to whom such information relates. On January 17, 2023, we received the results of this review and determined that the following types of information related to you were included in one or more files acquired by the unauthorized actor or present in one or more files that resided on an area of the ILS network that was accessed by the unauthorized actor: name, [Extra8][Extra9][Extra10]. Please note that we have no evidence or other indication that identity theft or fraud occurred as a result of this incident. We are providing this notice out of an abundance of caution.

What We Are Doing. We take this incident and the security of information entrusted to us very seriously. In response to the incident, we promptly took steps to mitigate any risk of compromise to your information and better prevent a similar event from reoccurring. These actions included: (1) fortifying the security of our firewall; (2) utilizing the forensic specialists engaged to monitor our network and remediate any suspicious activity identified; (3) rotating and increasing the complexity of all users’ credentials, and (4) providing notification to potentially affected individuals as quickly as possible. We are also enhancing our existing training protocols and other internal



procedures that relate to data protection and security. In accordance with best practices, we encourage you to review your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately.

As an added precaution, we are also providing you with access to [Extra7] months of complimentary identity monitoring and restoration services through Experian, along with guidance on how to protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. You can find out more about how to protect your information in the enclosed *Steps You Can Take to Protect Information*. There, you will also find additional details about the identity monitoring services we are offering and how to enroll.

For More Information. If you have questions about this incident that are not addressed in this letter, please contact our dedicated assistance line, which can be reached at 800-906-7238 toll-free Monday through Friday from 8 am - 10 pm Central, or Saturday and Sunday from 10 am - 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number [Engagement Number].

We apologize for any inconvenience this incident may cause you and remain committed to safeguarding the privacy and security of information in our possession.

Sincerely,

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

STEPS YOU CAN TAKE TO PROTECT INFORMATION

Enroll in Identity Protection Services

As an added precaution, we are offering complimentary access to Experian IdentityWorksSM for [Extra7] months. Please note that Identity Restoration is available to you for [Extra7] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra7] month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by July 5, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 800-906-7238 by July 5, 2023. Please be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY MONITORING SERVICES

A credit card is not required for enrollment in Experian IdentityWorks. 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.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 1-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

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.



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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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.

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 violator. 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 [X] Rhode Island residents impacted by this incident.





Return Mail Processing
PO Box 999
Suwanee, GA 30024

12 1 3002 *****SNGLP

SAMPLE A. SAMPLE - L02

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



March 14, 2023

NOTICE OF DATA [EXTRA6]

Dear Sample A. Sample:

Independent Living Systems, LLC (“ILS” or “We”) provides a variety of managed services to several partner health plans and their enrollees or referred individuals, including [Extra4]. ILS’s services include plan administration, nutrition support, and comprehensive care management. We are committed to protecting the confidentiality and security of the information we gather in providing these services.

We are writing to make you aware of a data incident that may impact the privacy of your personal information and/or protected health information (“PHI”). Please read this letter carefully, as it provides details about the incident and our response.

What Happened? On July 5, 2022, we experienced an incident involving the inaccessibility of certain computer systems on our network. We responded to the incident immediately and began an investigation with the assistance of outside cybersecurity specialists. Through our response efforts, we learned that an unauthorized actor obtained access to certain ILS systems between June 30 and July 5, 2022. During that period, some information stored on the ILS network was acquired by the unauthorized actor, and other information was accessible and potentially viewed. Upon containing the incident and reconnecting our computer systems, we began to review the potentially affected data to determine whether it contained any personal information or PHI, and if so, to whom such information related.

What Information Was Involved? As previewed above, we conducted a comprehensive data review exercise to understand the scope of potentially affected information and identify the individuals to whom such information relates. On January 17, 2023, we received the results of this review and determined that the following types of information related to you were included in one or more files acquired by the unauthorized actor or present in one or more files that resided on an area of the ILS network that was accessed by the unauthorized actor: name, [Extra8][Extra9][Extra10]. Please note that we have no evidence or other indication that identity theft or fraud occurred as a result of this incident. We are providing this notice out of an abundance of caution.

What We Are Doing. We take this incident and the security of information entrusted to us very seriously. In response to the incident, we promptly took steps to mitigate any risk of compromise to your information and better prevent a similar event from reoccurring. These actions included: (1) fortifying the security of our firewall; (2) utilizing the forensic specialists engaged to monitor our network and remediate any suspicious activity identified; (3) rotating and increasing the complexity of all users’ credentials, and (4) providing notification to potentially affected individuals as quickly as possible. We are also enhancing our existing training protocols and other internal



procedures that relate to data protection and security. In accordance with best practices, we encourage you to review your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately.

What You Can Do. You can find out more about how to protect your information in the enclosed *Steps You Can Take to Protect Information*.

For More Information. If you have questions about this incident that are not addressed in this letter, please contact our dedicated assistance line, which can be reached at 800-906-7238 toll-free Monday through Friday from 8 am - 10 pm Central, or Saturday and Sunday from 10 am - 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B086939.

We apologize for any inconvenience this incident may cause you and remain committed to safeguarding the privacy and security of information in our possession.

Sincerely,

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

STEPS YOU CAN TAKE TO PROTECT INFORMATION

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 1-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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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.

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 violator. 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 [X] Rhode Island residents impacted by this incident.