



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

August 29, 2024

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 WellLife Network Inc. ("WellLife"), located at 1985 Marcus Avenue, Suite 100, New Hyde Park, NY 11576, and are writing to notify your office of an event that may affect the security of certain information relating to approximately twelve (12) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, WellLife 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 September 7, 2023, WellLife became aware of suspicious activity in its network. WellLife promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between August 26, 2023 and September 7, 2023, an unauthorized actor gained access to certain WellLife systems and may have viewed or taken certain information contained therein.

WellLife conducted a thorough and in-depth review to identify what information was potentially accessible and to whom such information relates. WellLife completed its review on August 1, 2024, and then moved as quickly as possible to notify potentially affected individuals.

The investigation was not able to confirm the exact information that was actually accessed or taken during the event. However, the investigation determined that the following personal information related to Maryland residents was potentially accessible: name, address, Social Security number, driver's license, Passport, other government-issued identification (potentially including state ID, military ID, tribal ID, or taxpayer identification number), medical information (potentially including medical diagnosis/condition information, lab results, medications, and other treatment information), and health insurance information.

Notice to Maryland Residents

On August 29, 2024, WellLife mailed written notice of this event to potentially impacted individuals, including approximately twelve (12) Maryland 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 becoming aware of the event, WellLife moved quickly to investigate and respond to the event, assess the security of WellLife's network, and identify potentially affected individuals. As part of its ongoing commitment to information security, WellLife is reviewing its existing policies and procedures and implementing additional administrative and technical safeguards to further enhance its security posture. WellLife also notified federal law enforcement and is providing access to credit monitoring and identity restoration services for twelve (12) months, through Experian, to Maryland residents whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, WellLife 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, bank, or other applicable institution. WellLife 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.

WellLife is providing written notice of this event to relevant state regulators, as required, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. WellLife is also notifying the U.S. Department of Health and Human Services, posting notice on its website, and providing notice to prominent media in New York pursuant to the Health Insurance Portability and Accountability Act ("HIPAA").

Office of the Attorney General
August 29, 2024
Page 3

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 Freind of
MULLEN COUGHLIN LLC

AWF/aml
Enclosure

EXHIBIT A



Return Mail Processing
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

<<Variable Header/Var data 3>>

Dear <<Full Name>>:

WellLife Network Inc. (“WellLife”) writes to inform you of an event that may impact some of your information. You are receiving this letter because you or a family member <<Variable data 3 (relationship)>>. Although we have no indication of any actual or attempted identity theft or fraud as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On September 7, 2023, WellLife became aware of suspicious activity in its network. We promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between August 26, 2023 and September 7, 2023, an unauthorized actor gained access to certain WellLife systems and may have viewed or taken certain information. We conducted a thorough and in-depth review to identify what information was potentially accessible and to whom such information relates. We recently completed this process, and then moved as quickly as possible to notify potentially affected individuals.

What Information Was Involved? The investigation was not able to confirm the exact information that was actually viewed or taken during the event. However, the investigation did determine that your name, <<Breached Elements>> were potentially accessible to an unauthorized individual.

What We Are Doing. We take this event and information security very seriously. Upon becoming aware of the event, we moved quickly to investigate and respond to the event, assess the security of our network, and notify potentially affected individuals. As part of our ongoing commitment to information security, we are reviewing our existing policies and procedures and implementing additional administrative and technical safeguards to further enhance our security posture. We are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are offering credit monitoring and identity restoration services through Experian for <<CM Duration>> months, at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, credit reports, and explanation of benefits forms for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to your bank, credit card company, healthcare/insurance provider, or other applicable institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring and identity restoration services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-833-251-9580, Monday through Friday from 9:00 AM to 9:00 PM Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call. You may also write to WellLife at 1985 Marcus Avenue, Suite 100, Hew Hyde Park, NY 11042. Again, we take the privacy and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Sherry Tucker
Chief Executive Officer
WellLife Network Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for <<CM Duration>> months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for <<CM Duration>> 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 <<CM Duration>> -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** <<Enrollment Deadline>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<Activation Code>>

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 1-877-288-8057 by <<Enrollment Deadline>>. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR <<CM Duration>> -MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

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, 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.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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 <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<#>> Rhode Island residents that may be impacted by this event.