

Notification of Data Security Incident

Notification of Data Security Incident

June 11, 2026 – Lifeways, Inc. (“Lifeways”) has become aware of a data security incident that may have impacted information belonging to certain individuals. Lifeways is not aware of any evidence to suggest that any information has been misused.

On January 20, 2026, Lifeways discovered suspicious activity potentially related to an employee email account. Upon discovery, Lifeways took swift action to secure its email system and network. Lifeways then immediately began working with third-party computer specialists to investigate the full nature and scope of the incident. Based on the investigation, it was determined that a limited number of emails within certain employee email accounts were subject to unauthorized access. As a result, together with third-party specialists, Lifeways began a comprehensive and time-consuming review of the impacted emails to determine the type of information contained therein and to whom that information related.

This review was recently completed on May 8, 2026. Following the comprehensive and time-intensive analysis, Lifeways determined that information contained in the affected data set may have included protected health information (“PHI”). The type of information contained within the affected data set may include a first and last name, in combination with one or more of the following: date of birth, Social Security number, driver’s license or state identification number, financial account number, medical record number, medical diagnosis information, treatment location, clinical information, Medicare number, health insurance group number, medical treatment/procedure information, treatment location, prescription information, provider name, health insurance account number, Medicaid number, and/or patient account number.

At this time, Lifeways is not aware of any evidence to suggest that any information has been fraudulently misused. However, in an abundance of caution, Lifeways is notifying potentially impacted individuals of this incident. Although Lifeways has no reason to believe any individual’s information has been or will be misused as a result of this incident, individuals are nonetheless encouraged to monitor their account statements and explanation of benefits forms for suspicious activity and to detect errors.

Lifeways has established a toll-free number to answer questions about the incident and to address related concerns. The number to call is 1-800-405-6108 during 8:00 am to 8:00 pm ET, Monday – Friday, excluding major US holidays.

Lifeways takes the privacy and security of the information in its care seriously, and sincerely regrets any worry or inconvenience this incident may have caused.

What steps can I take to protect my private information?

- We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.
- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies appears at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identity theft. The FTC’s website offers helpful information at ftc.gov/idtheft.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies is included in the notification letter and is also listed at the bottom of this page.

How do I put a fraud alert on my account?

A fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

TransUnion

1-800-680-7289
www.transunion.com

Experian

1-888-397-3742
www.experian.com

Equifax

1-888-298-0045
www.equifax.com

TransUnion Fraud Alert

P.O. Box 2000
Chester, PA 19016-2000

Experian Fraud Alert

P.O. Box 9554
Allen, TX 75013

Equifax Fraud Alert

P.O. Box 105069
Atlanta, GA 30348-5069

TransUnion Credit Freeze	Experian Credit Freeze	Equifax Credit Freeze
P.O. Box 160	P.O. Box 9554	P.O. Box 105788
Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.