

## U.S. Vision Notice of Data Event

USV Optical, Inc., a subsidiary of U.S. Vision, Inc., (“U.S. Vision”) recently became aware of potentially suspicious activity on our computer network that may have impacted the security of certain information on those systems. With the assistance of third-party computer forensic specialists, we took immediate steps to contain the incident and to investigate the nature and scope of the incident. U.S. Vision is issuing this notice to provide additional details regarding what is known about the incident, the further steps we are taking in response, and steps potentially impacted individuals can take, if deemed appropriate.

**What Happened?** On May 12, 2021, U.S. Vision identified potentially suspicious activity involving our servers and systems. We began investigating the activity with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. This investigation confirmed there was unauthorized access to certain servers and systems between April 20, 2021 and May 17, 2021. That investigation is ongoing. However, the investigation determined that records related to certain customers and employees may have been viewed and/or taken by an unauthorized individual as a result of this incident. Therefore, U.S. Vision is notifying potentially impacted individuals that their information may have been at risk.

**What Information Was Involved?** While the investigation is ongoing, the information that may have been impacted by this incident includes individuals’ name, eyecare insurance information including policy and/or subscriber information, eyecare insurance application and/or claims information, and for a smaller number of individuals may include address, date of birth, and/or other individual identifiers. We have no evidence of any identity theft or fraud occurring as a result of this incident.

**What Is U.S. Vision Doing?** We take this incident and the security of information in our care seriously. Upon discovery, we launched an investigation and took steps to secure our systems. We worked diligently to investigate and respond to this incident and continue working to identify and notify potentially impacted individuals. We are also reviewing and enhancing existing policies related to data protection. We are reporting this incident to relevant state and federal regulators as required. Further, we are notifying potentially impacted individuals so that they may take further steps to help protect their information, should they feel it is appropriate to do so.

**What Can Affected Individuals Do?** While we have no evidence of identity theft or fraud occurring as a result of this incident, we encourage everyone to review the below, *Steps You Can Take to Help Protect Your Information*.

**For More Information.** We understand you may have additional questions concerning this incident. Individuals can direct questions to the telephone number 866-435-7111, during working hours: Monday through Friday from 8:30 am to 10:00 pm ET and Saturday from 9:00 am to 5:30 pm ET.

## *Steps You Can Take to Help Protect Your 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](http://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 security 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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-833-395-6938
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](http://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.