28470

<<Variable Text 3: Use image tied to text value>>

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-814-1705
Or Visit:
https://response.idx.us/incident-information
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

October 28, 2022

Su información personal puede haber estado involucrada en un incidente de datos. Si desea recibir una version de esta carta en español, por favor llame 1-833-814-1705.

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>:

We are writing to inform you of a data security incident that occurred at USV Optical, Inc., a subsidiary of U.S. Vision, Inc., ("U.S. Vision") and may have affected your personal information. Nationwide Optical Group, LLC acquired or became affiliated with several entities from U.S. Vision in September 2019, including <<Variable Text 2>>. Following this, U.S. Vision continued to provide us with some administrative services as a business associate to us. The records reviewed by U.S. Vision indicate that you may have received services from <<Variable Text 3>> at some point in the past.

What happened?

U.S Vision has represented to us that on May 12, 2021, U.S. Vision became aware of suspicious activity involving its computer network. U.S. Vision launched an investigation into the nature and scope of the incident with the assistance of cybersecurity specialists. Through its investigation, U.S. Vision learned that an unauthorized individual accessed its network intermittently between April 20, 2021 and May 17, 2021, and that files containing your information may have been viewed and/or taken by the unauthorized individual.

U.S. Vision informed us of this incident on May 12, 2021, but was unable to identify which entities or patients were affected by this incident. We immediately began communications with U.S. Vision to obtain more information regarding this incident and determine whether any of our patients were affected. We also insisted that U.S. Vision institute dark web monitoring for any potential <<Variable Text 3>> data that could have been involved in this incident. U.S. Vision did not report any instances of actual or attempted misuse of <<Variable Text 3>> information through its dark web monitoring.

In addition, U.S. Vision has represented that, with third-party support, it conducted a comprehensive review of the impacted files to determine what information was affected and to whom the information related. On September 22, 2022, we received confirmation from U.S. Vision that your personal information was involved in this incident. We then conducted additional data enrichment and validation to further confirm impacted individuals and their mailing addresses, and the entities with which such individuals were associated. This review was completed on October 17, 2022.

What information may have been involved?

Personal information involved in this incident may have included one or more of the following elements: (1) identifying information (such as full name, date of birth, and address); (2) Social Security number, taxpayer identification number, driver's license number, and/or financial account information; (3) medical and/or treatment information (such as medical record number, dates of service, provider name, diagnosis or symptom information, and prescription/medication); (4) health insurance information (such as payor and subscriber/Medicare/Medicaid number); and (5) billing and claims information. Please note that not all data elements were present for all individuals. <<Variable Text 4.>>

What we are doing.

U.S. Vision has stated that upon discovering the incident, it moved quickly to investigate and respond, assess the security of relevant U.S. Vision systems, and identify any impacted data. As part of its ongoing commitment to the security of information, U.S. Vision has stated that it is evaluating opportunities to improve security and to better prevent future events of this kind. We take privacy and security very seriously. This incident did not impact our systems or files—it occurred at and impacted only U.S. Vision systems and files. We have and continue to enhance our security controls and monitor our systems to ensure no similar activity occurs on our systems.

We have arranged to offer you credit monitoring and identity restoration services for a period of <<12/24>> months, at no cost to you. You have until January 28, 2023 to activate these services, and instructions on how to activate these services are included in the enclosed Reference Guide.

What you can do.

In addition to enrolling in complimentary credit monitoring and identity restoration services, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid. Any questionable charges should be promptly reported to the company with which the account is maintained.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit https://response.idx.us/incident-information, or call toll-free 1-833-814-1705. This call center is open from 6 AM – 6 PM Pacific Time, Monday through Friday, except holidays.

We sincerely regret that this incident occurred and apologize for any inconvenience this incident may have caused you.

Sincerely,

<<Image tied to variable text 6: VP or President>>
<<Text tied to variable text 6: VP or President>>

<<Image tied to variable text 7: VP or blank>>
<<Text tied to variable text 7: VP or blank>>

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the company with which you maintain the account.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual 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 ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in IDX Credit and Identity Monitoring Services

As a safeguard, you may enroll, at no cost to you, in an online credit monitoring and identity restoration service provided by IDX.

To enroll in this service, please call 1-833-814-1705 or visit https://response.idx.us/incident-information and follow the instructions for enrollment using the Enrollment Code provided above.

The monitoring included in the membership must be activated to be effective. You have until January 28, 2023 to enroll in these services. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of potential fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General, and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

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 against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	1- 888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.

For Residents of Massachusetts

You have the right to obtain a police report with respect to 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.