Data Breach Notification

Name of Entity	U.S.Vision, Inc.,
Address of Entity	1 Harmon Drive Blackwood, New Jersey 08012
Contact Person	Rebecca L. Rakoski, Esquire XPAN Law Partners
Function of Contact Person	Outside Counsel
Postal Address of Contact Person	4 N Maple Avenue Marlton, New Jersey 08053
Email Address of Contact Person	rrakoski@xpanlawpartners.com
Phone Number of Contact Person	(267) 388-0897
Type of Breach	Ransomware, through a vulnerability in Microsoft's Exchange Server.
Date Ransomware Deployed	April 20, 2021
Date Discovered	May 12, 2021
Type of Data Potentially Impacted	First Name Last Name Date of birth Internal billing ID Carrier code Plan code Optometrist last name Eyewear insurance billing information
Impact to Data Subjects	Moderate
Credit Monitoring	None. Social security numbers are not collected by U.S.Vision.
Number of Data Subject Impacted	1,525 in Iowa.

	412,565 total data subjects affected.
Notification to Data Subjects	Notice on USV Website: September 3, 2021-Present Written mailed notice is in process.
Notification to Office of Civil Rights	September 3, 2021
Description of Data Breach	On May 12, 2021, USV's information technology department ("IT Department") received an alert that certain servers were not responding. Upon receiving these alerts, the IT Department began to investigate the issue and ultimately determined sixty-seven (67) servers were encrypted, including three (3) on-premises Microsoft Exchange Servers. The threat actor group, Conti, sent a ransom note. USV engaged outside legal counsel and a cyber-forensic company to investigate the Incident and restore the servers. The servers that were part of the Incident contained emails and unstructured data stored by both USV and an unaffiliated organization Nationwide. Despite the ransom demand, USV was able to eventually restore the servers without paying the cyber criminals. In early March 2021, large-scale worldwide cyber-attacks and data breaches were occurring resulting from zero-day exploits that were discovered within on-premises Microsoft Exchange Servers. The vulnerability gave threat actors unauthorized full administrative privileges on affected servers and connected devices on the same network. The nature of the vulnerability was such that the threat actors were able to install a backdoor that allowed full access to impacted servers even if the server is later patched/updated to no longer be vulnerable to the original exploits. It has been estimated that 250,000 servers, including servers belonging to around 30,000 organizations in the United States, were the victims of this issue.

	After 2 years of investigation, USV believes that due to the timeframe of the Incident and the nature of the attack, its servers were a victim of the Microsoft vulnerability. While this vulnerability was known to Microsoft as early as January 2021, it was not made public until March 2, 2021. At that time, Microsoft released updates for Microsoft Exchange Server to patch the exploit, but not only was the initial patch ineffective against the vulnerability, it also did not remove any backdoors previously installed by the attackers. In short, once the threat actor was in, the patch was ineffective to any already-impacted server. During the course of this cyber-investigation, USV's hired forensic experts who were able to trace web shell activity between March 4, 2021 and March 6, 2021, which corresponds to the timeframe when the Microsoft Exchange Server exploit was known but not yet addressed by Microsoft. USV took immediate action to implement any patch pushed out by Microsoft, but due to the timeframe of the web shell activity, the current working theory is that Conti was already in the servers. Accordingly, there was nothing USV could have done to prevent the Incident. At the time of the Incident, USV's existing proactive cybersecurity program could not have prevented this type of vulnerability and exploitation.
USV's IT Security and Subsequent Mitigation Efforts Post Breach	USV took immediate steps to address the data incident, as outlined more specifically above. Subsequent to the Incident, USV took additional measures to harden the security of its IT infrastructure. Those measures include, but are not limited to the following: 1. Implemented Proofpoint for email protection controls

	2. Installed and utilizes the advanced EDR, SentinelOne, on all endpoints. 3. Added Okta MFA for remote access. 4. Implemented a more robust data retention and destruction policy that deleted all files older than five years from its shared drives. 5. Cobalt pen testing and remediation. 6. Reviewed and updated its Incident Response Plan.
Additional Facts Related to Investigation	Due to the nature and scope of the affected data and servers, USV spent two (2) years attempting to determine the type of data impacted by the incident. As a result, it was not until recently that USV determined the individuals that required notice under HIPAA.

U.S.VISION

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>> <<Date>>
<<City>>, <<State>> <<Zip>>

Re: NOTICE OF DATA BREACH

Dear <<Name 1>> <<Name 2>>:

U.S. Vision, Inc. ("U.S. Vision") is writing to inform you of an event that may impact the privacy of some of your information. While we have no indication of any identity theft or fraud occurring as a result of this incident, we are providing you information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On May 12, 2021, U.S. Vision became aware of suspicious activity involving our computer network. We immediately launched an investigation into the nature and scope of the incident with the assistance of industry-leading cybersecurity specialists. Through the investigation, we learned that an unauthorized individual accessed our 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.

With third-party support, we then conducted a comprehensive review of the impacted files in order to determine what information was affected and to whom the information related. Given the unstructured and condensed nature of the accessed files, significant time was needed to review the accessed files and to identify any potentially affected individuals. Upon completion of the third-party review, we then conducted a manual review of our records internally to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications.

What Information Was Involved? Personal information involved in this incident may have included one or more of the following elements: (1) identifying information (such as first/last name, date of birth, address, telephone number and gender); (2) vision care and/or treatment information (such as record number, dates of service, provider name, and diagnosis code information); (3) vision care insurance information (such as payor and subscriber/Medicare/Medicaid number); and (4) billing and claims information. Please note that not all data elements were present for all individuals.

What We Are Doing. Upon discovering this incident, we moved quickly to investigate and respond, assess the security of relevant U.S. Vision systems, and identify any impacted data. We are continuously evaluating opportunities to improve security and to better prevent future events of this kind.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, and to review your account statements, explanation of benefits forms, and credit reports for suspicious activity. You may also review the information contained in the attached Steps You Can Take to Help Protect Your Personal Information.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. Should you have any questions, you may contact us at 866-435-7111 which can be reached Monday through Friday from 8:30 a.m. to 9:00 p.m. and Saturday 9:00 a.m. to 5:30 p.m. (Eastern Time).

Loyalty Reward. As a thank you for being our loyal customer we offer the enclosed **$25 Loyalty Reward**. The reward can be redeemed at any of the listed participating retailers through **December 31, 2024.**

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

Sincerely,

U.S. Vision, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL 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 fraud alert or 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	1-833-395-6938
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; 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: 441 4th St. NW #1100 Washington, D.C. 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. U.S. Vision, Inc. is located at 1 Harmon Drive, Blackwood, NJ 08012

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 1,243 Rhode Island residents impacted by this incident.

For Massachusetts residents, under Massachusetts law, you have the right to obtain any police report filed in regard 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.