



Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202
IDTheft@oag.state.md.us

September 29, 2022

Notice of Data Breach

To Whom It May Concern:

On behalf of VisionWeb Holdings, LLC ("VisionWeb"), an eye care practice management software provider, I am writing to inform you about an incident in which personal information relating to Maryland residents may have been accessed by an unauthorized third party.

We discovered a security incident in which an unauthorized third party gained access to a VisionWeb email account, which contained personal information related to certain VisionWeb employees and the patients of certain VisionWeb business customers (eye care practices in various U.S. states). After becoming aware of this access, we launched an investigation and began working with external cybersecurity experts to determine the scope of the incident, restrict access to this email account and ensure that the incident was contained. We also notified the Federal Bureau of Investigation. Through our investigation, we determined that the unauthorized access began on September 21, 2021 and ended on December 7, 2021. We also determined that the unknown third party could have accessed the names, health insurance information, patient identification numbers, and health information, including, treatment information of certain VisionWeb employees and business customers' patients. VisionWeb found no evidence to suggest that individual or employee data was actually accessed, acquired, or misused or that personal information was targeted by the unauthorized third party.

Please note that this incident required an extensive data review and business customer notice process. We worked diligently to review the affected data, determine what personal information was impacted and identify the individuals to whom it related. We then had to match the impacted patients to VisionWeb's business customers. Once we identified these customers, we notified them and offered to provide notice on their behalf to their impacted patients and any applicable regulators, including the Department of Health and Human Services. Because VisionWeb did not have access to the impacted patients' address information, customers who opted in to having VisionWeb give notice had to locate and provide their patients' mailing address information to enable us to send the required notices – and this process took time. Attached to this letter is a list of the practices on whose behalf we are notifying patients in Maryland. Also attached is a sample of the letter that we are providing to Maryland residents.

Please note that VisionWeb maintains a written information security program. In response to this incident, we took several steps consistent with our incident response protocols, including, but not limited to, disabling the compromised account, enhancing email password complexity requirements, and reviewing permissions for sensitive and restricted data. We will notify 3 Maryland residents of this incident on September 30, 2022.

Please know that we take our data protection responsibilities very seriously and we regret that this incident occurred. If you have any questions, please do not hesitate to contact me at (214) 289-0166. I can also be reached at 6500 River Place Blvd. Building 7, Suite 250 Austin, Texas 78730 and godom@visionweb.com.

Sincerely,

Nicolas Sinet

Nicolas Sinet
Chief Executive Officer, VisionWeb

Practices on Whose Behalf VisionWeb is Notifying Patients in Maryland

- Elite Vision Care PLLC
- Fort Myers Eye Associates PA
- MOA Medical Practices PC



VisionWeb Holdings, LLC
6500 River Place Blvd.
Building 7, Suite 250
Austin, Texas 78730

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

On behalf of VisionWeb Holdings, LLC (“VisionWeb”), I am writing to inform you about an incident that may have involved personal information about you. We regret that this incident occurred and take the security of your personal information seriously.

WHAT HAPPENED. VisionWeb provides eye care providers with practice management software and technology services. On December 9, 2021, VisionWeb learned that from September 21, 2021 to December 7, 2021, an unauthorized third party had access to a VisionWeb email account, which contained certain information belonging to VisionWeb’s business customers, including <<b2b_text_1(ProviderName)>>.

We are notifying you because you are a current or former patient of the above provider and some limited categories of personal information related to you may have been accessed by the unauthorized third party. Although we have identified no evidence that your data was actually accessed or misused and our investigation indicates that personal information was not targeted by the unauthorized third party, we are providing you with notice out of an abundance of caution.

WHAT WE ARE DOING. Please know that as soon as we became aware of the incident, we launched an investigation to determine the scope of the incident, notified federal law enforcement, took measures to restrict access to this email account, and evaluated our security practices. We also engaged in extensive data discovery to identify any impacted information and the providers to whom such information belonged.

WHAT INFORMATION WAS INVOLVED. The personal information that could have been accessed by the unauthorized third party includes your name and the following categories of personal information: <<b2b_text_2 (“name” and data elements)>>.

WHAT YOU CAN DO. We are providing you with the following information about steps that individuals can take to help protect against potential misuse of personal information.

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s Web site, at <https://www.identitytheft.gov/#/>, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com/personal/credit-report-services

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com/help

TransUnion
(888) 909-8872
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022
www.TransUnion.com/credit-help

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

You can also contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION. Please know that we take the security of your personal information seriously and regret any inconvenience that this incident may cause you. If you have any questions or concerns, please do not hesitate to contact us by calling toll free at (855) 544-2814. Representatives are available to provide assistance 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Nicolas Sinet

Nicolas Sinet
Chief Executive Officer, VisionWeb

State-Specific Information

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<http://www.identitytheft.gov>

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
<https://oag.dc.gov/>

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

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

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.com>

IF YOU ARE A RHODE ISLAND RESIDENT: We are notifying 19 Rhode Island residents of this incident. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
<http://www.riag.ri.gov/>