

May 2, 2024

425 rabro drive

hauppauge ny 11788

voice 800.645.3733

fax 800.228.6329

www.cvoptical.com

By Email: idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data Incident Notification¹

Dear Sir or Madam:

We are writing to notify your office that, on March 6, 2024, ClearVision Optical (“CVO,” or the “Company”) became aware of potential unauthorized activity on its systems (the “Incident”). The Company immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, CVO determined that the Incident resulted in the encryption of certain files stored on the Company’s information systems. The Company spent significant time and resources determining whether those files contained personally identifiable information (“PII”) and identifying the individuals to whom that PII related.

On or about April 8, 2024, the Company determined that, on or about March 6, 2024, files containing PII related to two (2) Maryland residents may have been accessed by the unauthorized party. Out of an abundance of caution, and in accordance with applicable law, notice will be provided to the affected Maryland residents, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused.

As set forth in the enclosed letter, CVO took a number of steps to mitigate the risk that the Incident would result in harm and to further bolster its data security program. Those steps include: enhancing the security of its email system, contracting with a cybersecurity company to provide endpoint detection and response services, and continuing to invest in updating technology equipment and software, including by utilizing cloud-based tools as appropriate. Additionally, CVO continues to enforce requirements related to multi-factor authentication, complex passwords, and where feasible, file encryption.

We will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me at (631) 787-1741.

Sincerely,



Jennifer Trakhtenberg
Co-Chief Operating Officer
Chief People Officer
ClearVision Optical



425 Rabro Drive, Suite #2
Hauppauge, NY 11788

May 2, 2024

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

We are writing to provide additional information regarding the system outage that ClearVision Optical (“CVO”) recently experienced, which resulted from unauthorized access to our network (the “Incident”). The Company immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, CVO determined that the Incident resulted in the encryption of certain files stored on the Company’s information systems. CVO spent significant time and resources determining whether those files contained personally identifiable information (“PII”) and to identify the individuals to whom that PII related.

On or about April 8, 2024, CVO determined that, on or about March 6, 2024, the system was compromised and the unauthorized party may have accessed PII that related to you in the affected systems. The Company has not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

The impacted files may have contained your name, along with your social security number.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information could be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identity theft protection services through CLC, a provider of identity theft solutions. These services include <<#Months>> months of credit monitoring and assisted ID theft recovery services. With this protection, CLC will help you resolve issues if your identity is compromised.

We encourage you to contact CLC with any questions and to enroll in free identity protection services by completing the online enrollment that has been emailed to you via the welcome letter. CLC does include 24/7 emergency customer service, however CLC representatives are available Monday through Friday from 11am EST – 8pm EST. Please note the deadline to enroll is July 15, 2024.

CVO treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. As part of its ongoing commitment to data security, CVO has and will continue to assess and implement upgrades to its data security program. For instance, it has enhanced the security of its email system, contracted with a cybersecurity company to provide endpoint detection and response services, and continued to invest in updating technology equipment and software, including by utilizing cloud-based tools as appropriate. Additionally, CVO continues to enforce requirements related to multi-factor authentication, complex passwords, and where feasible, file encryption.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We apologize for any inconvenience this Incident may have caused you and appreciate your support throughout the prior period of business disruption. If you have additional questions, email Jen at Jtrakhtenberg@cvoptical.com or Ann Marie at Atheologitis@cvoptical.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jen Trakhtenberg', with a stylized, cursive script.

Jennifer Trakhtenberg

Co-Chief Operating Officer
Chief People Officer
ClearVision Optical

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
800-685-1111
securitymonitoring@equifax.com

Experian
Experian Security Assistance
P.O. Box 9554
Allen, TX 75013
888-397-3742
businessrecordsvictimassistance@experian.com

TransUnion
Consumer Relations & Fraud
Victim Assistance
P.O. Box 2000
Chester, PA 19016
800-916-8800.
databreach@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue NW
Washington, DC 20580
4. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.
5. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State’s Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
6. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.
7. *For Oregon Residents:* You can obtain information about steps you can take to help prevent identity theft from the Oregon Department of Justice at: [Identity Theft - Oregon Department of Justice: Consumer Protection \(state.or.us\)](http://IdentityTheft-OregonDepartmentofJustice.ConsumerProtection(state.or.us)).