

20 Church Street
20th Floor
Hartford, CT 06103
Telephone: 860-525-5065
Fax: 860-527-4198
www.lockelord.com

Theodore P. Augustinos

June 11, 2021

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Hoya Optical Labs of America, Inc.
Notice pursuant to N.H. Rev. Stat. § 359-C:19

Dear Attorney General Formella:

We represent Hoya Optical Labs of America, Inc. ("Hoya"), a manufacturer of optical products. On behalf of Hoya, we hereby provide notice pursuant to N.H. Rev. Stat. § 359-C:19 of a security incident involving disclosure of the personal information of approximately 4 New Hampshire residents, based on our investigation to date.

What Happened

On April 5, 2021, Hoya discovered that files on some of its servers and workstations in the U.S. had been encrypted in an apparent ransomware attack. Hoya immediately terminated the attack and began to investigate. Hoya engaged our law firm, and we engaged experienced outside forensics investigators to determine the scope and nature of the attack, as well as the extent to which the security of personal and corporate information may have been compromised. The investigation could not establish the first point or time of access by the attacker, but activity was discovered as early as March 15, 2021. The investigation determined that the last evidence of threat actor activity took place on April 5, 2021. Hoya learned on April 23, 2021 that the attackers published the information they had claimed to have stolen. Hoya subsequently expanded its team of professionals to collect and review the data published by the attackers as thoroughly and quickly as possible.

What Information Was Involved

Based on Hoya's investigation, which is ongoing, it appears that the personal information exposed in this incident included affected individuals' names, addresses, personal e-mail addresses and telephone numbers, Social Security numbers, payroll information (including financial account information), personal payment card number and details, certain health and medical information, and driver's license number. Not all affected individuals had the same types of information compromised.

June 11, 2021
Page 2

What Hoya Is Doing

As noted above, immediately upon the discovery of the attack, Hoya took steps to terminate it and prevent any further unauthorized access. As required by N.H. Rev. Stat. § 359-C:20(I), Hoya is providing notice of this incident to the affected individuals by mail on or about June 11, 2021. A template for the notification letter is attached. The notification letter describes Hoya's offer of credit monitoring services for 2 years at no cost to the affected individuals, and provides additional guidance for affected individuals to protect themselves. Hoya is also reviewing and enhancing its safeguards to mitigate the risk of further or future compromises of personal information.

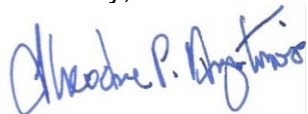
On behalf of Hoya, we are notifying state agencies as required in jurisdictions where affected individuals reside.

Please note that the investigation is ongoing and Hoya expects to notify additional populations as to other types of data upon completion of the data review process. At that time, if appropriate, we expect to supplement this notification.

* * * * *

Please do not hesitate to contact me with any questions related to this matter.

Sincerely,



Theodore P. Augustinos

Enclosure



Logo

C/O [VENDOR]

<<Return Address>>

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

<<First Name>> <<Last Name>>

<<Address 1>> <<Address 2>>

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

To Enroll, Please Call:
[insert toll-free number]
Or Visit:
[VENDOR WEBSITE]
Enrollment Code: [XXXXXXXXXX]

<<Date>>

Re: Notice of Data Breach

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

Hoya Optical Labs of America, Inc. is contacting you about a recent ransomware cyber-attack that is further described below. We are notifying you of this incident and providing you with tools and guidance to help you protect yourself against potential risk of identity theft and fraud. If our investigation determines that members of your household or other dependents were also affected by this incident, they will receive separate letters.

What Happened

On April 5, 2021, we discovered that files on some of our servers and workstations in the U.S. had been encrypted in an apparent ransomware attack. Our team worked diligently to minimize the impact on our servers and operations, and to restore functionality. We engaged an outside law firm and forensics experts to investigate the scope and impact of the incident, including investigating whether any data was taken by the attackers. Based on our investigation, which is ongoing, your personal information may have been acquired by the attacker. We learned on April 23, 2021 that the attackers published the information they had claimed to have stolen. We have expanded our outside team of experienced professionals to collect and review the data published by the attackers as thoroughly and quickly as possible. Although our review of the information is still ongoing, it appears that it may include some Social Security numbers, and potentially other personal information. We are notifying you of this incident, and providing you with services and guidance to help you protect yourself in an abundance of caution. We describe the available services below.

What Information Was Involved

We are thoroughly analyzing the data that had been compromised, but based on our investigation, which is ongoing, it appears that this event may have compromised the security of some or all of the following data: your name, address, personal email address and telephone number, Social Security number, payroll information including your financial account for direct deposit, username and passwords to your financial and/or online accounts, certain health and medical information, personal payment card number and details, and driver’s license number.

What We Are Doing

Immediately upon learning of the problem, we began reviewing all aspects of the incident, and taking steps to protect the systems and everyone involved. We are working closely with outside experts to address the incident properly. We reported the incident to law enforcement. We are also reviewing and enhancing our system security, governance practices and ongoing monitoring to help prevent a recurrence of an incident like this in the future.

In addition, we are covering the full cost to offer you identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you monitor and resolve issues if your identity is compromised.

What You Can Do

As always, we recommend that you remain vigilant and review your account statements and credit reports regularly, and report any concerning transactions to your financial services provider.

We encourage you to contact IDX with any questions and to enroll in identity protection services we are providing at no cost to you by calling [TFN] or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is [Enrollment Deadline].

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call [insert VENDOR toll-free number] or go to [VENDOR WEBSITE] for assistance or for any additional questions you may have.

Sincerely,

Shelley Harvey
VP of HR, Americas Region

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your **IDX** identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, **IDX** will be able to assist you.

3. Telephone. Contact **IDX** at [\[insert IDX toll-free number\]](#) to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in **IDX** identity protection, notify them immediately by calling or by logging into the **IDX** website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our **ID Care team** who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an **ID Care Specialist** who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document.

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 agencies 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 a 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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392, State law advises you to report any suspected identity theft to law enforcement, as well as the FTC.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.