

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
scottkev@gtlaw.com

January 13, 2022

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

We are writing to inform you that our client, Millennium Eye Care, LLC (“MEC”), located at 500 W Main St, Freehold, NJ 07728, has notified 2 Maryland residents of a data security incident that may have impacted some of their personal information.

MEC was recently the target of a sophisticated computer attack. The attacker gained access to MEC’s IT systems, holding those systems hostage with the goal of extorting money to prevent the disclosure of personal information. MEC took immediate action to isolate the attack, investigate, and secure its IT environment. MEC also reported the attack to law enforcement. MEC’s investigation revealed that the personal information of current and former patients was accessed by the attackers. On November 15, 2021, MEC discovered that the attackers exfiltrated some data which included patient names, addresses and procedure lists.

A copy of the notification letter mailed on January 13, 2022 is attached.

MEC takes the security of its information seriously and has taken measures to reduce the likelihood of a future cyber-attack, including increased network security measures and employee training to recognize external attacks.

Please contact me for any additional information.

Best Regards



Kevin M. Scott

Attachment



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

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

January 13, 2022

Dear <<FirstName>> <<LastName>>,

We are writing to notify you of a recent data security incident that may have impacted some of your personal information. We take the security of your information very seriously, and we sincerely apologize for any concern this incident may cause. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?

As you may be aware, we were recently the target of a sophisticated computer attack. The attacker gained access to our IT systems, holding those systems hostage with the goal of extorting money to prevent their disclosure of information. We took immediate action to isolate the attack, investigate, and secure our IT environment. We also reported the attack to law enforcement.

What Information Was Involved?

On November 15, 2021, we discovered that the attackers exfiltrated some data which included, among other things, personal information including your name, address, and procedure lists. **Your Social Security number and financial information were not accessed and remain secure.**

What We Are Doing

We take the security of your information seriously and have taken measures to reduce the likelihood of a future cyber-attack, including increased network security measures and employee training to recognize external attacks to meet the continually evolving cyber threat.

What You Can Do

Although we have no reports of misuse of your or anyone's information, we encourage you to review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection.

For More Information

If you have any questions, please call 1-833-381-2284 Monday through Friday from 9:00 am – 9:00 pm Eastern Time, excluding major U.S. holidays. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink that reads 'Steven K. Mishkin'.

Steven K. Mishkin, M.D.

(Enclosure)

Important Additional Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights pursuant to the federal Fair Credit Reporting Act. Please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General

441 4th Street NW
Washington, D.C.
20001
1-202-727-3400
www.oag.dc.gov

Maryland Office of Attorney General

200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of Attorney General

150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Attorney General

9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
www.ncdoj.com

New York Attorney General

120 Broadway
3rd Floor
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze for yourself or your spouse or a minor under 16: (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; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
<https://www.experian.com/help/>
1-888-397-3742

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/> 1-800-525-6285

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016-0200
<https://www.transunion.com/credit-help>
1-800-680-7289