



Freeman
Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Robert H. Bender, Jr.
Senior Counsel
D: 215.650.6619
Robert.bender@fmglaw.com

This submission is provided pursuant to the Maine Data Breach Notification Statute of 2019, ME. REV. STAT. § 1348(5). By providing this notification, Smart Vision and Smart Holdings LLC dba Smart Eye Care does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

In May 2023, Smart Eye Care learned of unusual activity within an employee's mailbox, which it promptly investigated. Smart Eye Care promptly investigated this activity and determined an unauthorized actor had accessed the employee's email account between April 27 and May 3, 2023. Smart Eye Care conducted a comprehensive review of the mailbox to identify what information was present and to whom the information related. The investigation identified unauthorized access to one employee email account on separate occasions beginning on April 27, 2023, until May 3, 2023. Smart Eye Care therefore performed a thorough review of the potentially accessed emails to identify what information was present during and to whom the data related so it could notify applicable individuals. On June 16, 2023, Smart Eye Care completed this review. The types of personal information impacted include name, address, and Social Security number.

On June 30, 2023, Smart Eye Care provided notice via U.S. regular mail of the incident to two Maine residents. A sample copy of the notice is attached as **Exhibit "A"** for your records. As an added precaution, Smart Eye Care offered affected individuals 12 months of complimentary credit monitoring and identity restoration services through IDX. The notice to the affected individuals also includes instructions on the use of this product as well as encouragement to remain vigilant for incidents of fraud or misuse and guidance on how to protect against identity theft and fraud, including information on how to place a fraud alert and/or security freeze. It also included the contact details for the national consumer reporting bureaus, and encouragement to contact law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered.

After discovering the incident, Smart Eye Care reset passwords to all relevant email accounts. In addition, Smart Eye Care continues to review its policies and procedures for ways to enhance the existing protections it has in place for its organization.

If you have questions about this notification or the data security event, please contact us at 215-650-6619.

Exhibit “A”



484 Maine Avenue
Suite 1
Farmingdale, ME 04344

To Enroll, Please Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code:
[REDACTED]

[REDACTED]
[REDACTED]

Dear [REDACTED]:

Smart Vision LLC and Smart Holdings LLC d/b/a Smart Eye Care values the privacy and security of your information, which is why we are notifying you of a recent incident that may involve some of your information. This letter provides a summary of the event, our response, and steps you can take to protect your information, should you feel it appropriate to do so. We are also providing you with access to complimentary identity monitoring and protection services at no cost. Enrollment instructions are included with this letter.

What Happened? Smart Eye Care recently learned of suspicious email activity involving an employee email account. Smart Eye Care commenced an investigation into the activity and identified unauthorized access to one employee email account at various times between April 27 and May 3, 2023 by someone outside our organization. We conducted a comprehensive review of the mailbox to identify what information was present and to whom the information related. We are notifying you because on June 16, 2023 our investigation concluded your information was present in the mailbox during the window of unauthorized access; however, we were unable to confirm if any of your information was viewed by the unauthorized actor.

What Information Was Involved? You are receiving this letter because, based on our review, information including your name, address, and Social Security number was present within emails and attachments accessed by someone outside our organization.

What We Are Doing? We take the privacy and security of personal information entrusted to us very seriously. Upon discovery of the incident, we reset passwords to all user accounts and implemented multi-factor authentication to prevent future unauthorized access. We continue to review our policies and procedures for ways to enhance the existing protections we have in place for our organization.

As an additional precautionary measure to help protect your information, we are offering you a complimentary one year of complimentary credit monitoring and identity restoration assistance from IDX. The offered services include: CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

What You Can Do. We encourage you to remain vigilant for incidents of fraud or misuse by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or issuing bank immediately, along with law enforcement. Please refer to the enclosed documentation titled *Steps to You Can Take to Help Protect Information* for contact information and resources you may take advantage of to protect against fraud or misuse, should you find it appropriate to do so.

Additionally, you may enroll in free IDX identity protection services by going to <https://app.idx.us/account-creation/protect> or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Standard Time. Please note the deadline to enroll is **February 01, 2024**.

For More Information. If you have additional questions, please call contact Smart Eye Care at 207-622-5800 (Augusta location), 207-947-7554 (Bangor location), or 207-582-5800 (Farmingdale location) during regular business hours.

Sincerely,

Smart Eye Care

STEPS TO YOU CAN TAKE TO HELP PROTECT INFORMATION

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. 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 (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, you should report any incorrect information on your report to the credit reporting agency.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as suffixes);
2. Social Security number;
3. Date of birth;
4. Address 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;
7. A copy of any police report, investigative report, or complaint to law enforcement concerning identity theft if you are a victim of identity theft.

To place a fraud alert or credit freeze, please contact the three major consumer reporting bureaus:

Equifax
1-888-298-0045
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

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

TransUnion
1-800-916-8800
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Report suspected fraud. 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 should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.