

February 5, 2024

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
ATTN Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy Brooks Smith & Prophete LLP represents Eyman Associates, P.C. ("Eyman Associates") in connection with a recent data security incident described in greater detail below.

1. Nature of the security Incident.

On November 30, 2023, Eyman Associates identified suspicious activity associated with one employee email account. In response, Eyman Associates took immediate steps to secure its email environment and promptly launched an investigation. Eyman Associates also engaged independent cybersecurity experts to conduct an investigation. As a result of this investigation, Eyman Associates learned that an unauthorized actor accessed certain data stored within the email account. After a thorough review of the accessed data, on January 23, 2024, Eyman Associates determined that certain personal information may have been impacted by this incident.

Please note that Eyman Associates has no evidence of the misuse or attempted misuse of any potentially impacted information. The information that may have been accessible by the malicious actor(s) responsible for this incident includes an individual's name and Social Security Number.

2. Number of Maryland residents affected.

Eyman Associates notified one (1) Maryland resident of this incident via first class U.S. mail on February 5, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Eyman Associates learned of this incident, Eyman Associates took steps to evaluate the potentially affected data and determine whether any personal or protected health information was affected. Out of an abundance of caution, Eyman Associates is also providing complimentary identity protection services to the affected individual.

4. Contact information.

Eyman Associates remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Best regards,

A handwritten signature in black ink, appearing to read "L. Nickle".

Lindsay B. Nickle
Partner

Enclosure: Sample Notification Letter

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: [REDACTED]

Subject: Notice of Data Security Incident

February 5, 2024

Dear [REDACTED]:

We are writing to inform you of a recent data security incident experienced by Eyman Associates, headquartered in Washington, D.C., that may have involved some of your information. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened: On November 30, 2023, Eyman Associates identified suspicious activity associated with one employee email account. In response, Eyman Associates took immediate steps to secure its email environment and promptly launched an investigation. Eyman Associates also engaged independent cybersecurity experts to conduct an investigation. As a result of this investigation, Eyman Associates learned that an unauthorized actor accessed certain data stored within the email account. After a thorough review of the accessed data, on January 23, 2024, Eyman Associates determined that your personal information may have been impacted by this incident.

There is no evidence that your personal information has been misused. However, out of an abundance of caution, we are notifying you about the incident, providing you with resources to help you protect your personal information, and offering you complimentary identity protection services.

What Information Was Involved: The data that could have potentially been accessed by the unauthorized party included your name and Social Security Number.

What We Are Doing: To help prevent something like this from happening again, we are implementing additional technical security measures. We are also providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are offering you 12 months of complimentary identity monitoring services through IDX. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do: You can follow the recommendations included with this letter to help protect your information. In addition, you can also enroll in IDX's complimentary credit and identity monitoring services by going to the link noted above or calling the number noted above. When prompted, please provide the unique code noted above to enroll in the services. The deadline to enroll is May 5, 2024. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: If you have any questions regarding the incident, please call 202-567-6203 Monday through Friday, between 9am and 5pm EST.

The security of the information in our possession is a top priority for Eyman Associates. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Barbara Eyman, Principal

Eyman Associates, PC
300 New Jersey Ave. NW
Suite 900
Washington, D.C. 20001

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>