ASSETMARK

November 7, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

RE: **Notice of an Incident – Maryland Personal Information Protection Act ("PIPA")**

To Whom it May Concern:

AssetMark, Inc. ("AssetMark") hereby provides notice of an incident that involved personal information of one Maryland resident, pursuant to the PIPA.

Description of Security Breach

On October 21, 2024, an unauthorized third party accessed the email accounts of two AssetMark employees and viewed the Personal Information of one Maryland resident ("Incident"). AssetMark detected this activity and immediately took steps to terminate the unauthorized access. An investigation was promptly launched by our Information Security Team.

Number of Maryland Residents Being Notified

AssetMark will notify the one Maryland resident whose personal information was accessed during this Incident, by sending the attached notice.

What Information Was Compromised

The unauthorized third party may have had access to the following information: name, address, phone number, AssetMark account number and social security number. Please note this incident did not involve access to the Maryland resident's AssetMark account(s).

The Steps AssetMark is Taking to Restore the Integrity of the System

We take this incident and the security of client information very seriously. Upon detecting this activity, AssetMark promptly took steps to terminate the unauthorized access. Additionally, AssetMark:

- Automatically disabled compromised user accounts, upon detection by our security tools, and passwords were reset before re-enabling those users accounts.
- Reviewed logs to determine that access by the unauthorized third party was limited to certain emails within two email accounts and no other AssetMark systems.
- Multi-factor authentication (MFA) policies have been further enhanced
- Noted the Maryland resident's account(s) with internal fraud warnings as a safety precaution

ASSETMARK

We are also providing, at no cost to the Maryland resident, a two-year subscription to ID Shield, a credit monitoring service.

For More Information

For more information, you may contact Jim Attaway, Senior Vice President, Infrastructure and Chief Information Security Officer, at jim.attaway@assetmark.com.

Sincerely,

Claire Blue

Claire Blue
Chief Compliance Officer
AssetMark, Inc.
claire.blue@assetmark.com

Attachment

ASSETMARK

November 7, 2024

CLIENT
ADDRESS

RE: **Notice of a Breach of Security**

Dear CLIENT:

We, AssetMark, Inc. ("AssetMark"), are contacting you to notify you of an incident that involved your personal information. We take the security of your information very seriously and are reaching out to let you know what happened and the steps we have taken and to provide you with additional information and services that may be helpful to you.

What Happened

On October 21, 2024, an unauthorized third party breached AssetMark's security ("Incident"). AssetMark detected this activity and immediately took steps to terminate the access. An investigation of this Incident was promptly launched by our Information Security Team.

What Information Was Compromised

The unauthorized third party may have had access to personal information, including your name, address, phone number, AssetMark account number and social security number.

Please note this Incident did not involve access to your AssetMark account(s).

What We Are Doing

We take this Incident and the security if your information very seriously. As noted above, upon detecting this activity, we promptly took steps to terminate the activity and address the Incident.

- Compromised user accounts were automatically disabled upon detection by our security tools. Passwords were reset before re-enabling the users accounts.
- AssetMark reviewed logs to determine that access by the unauthorized party was limited to email and no other AssetMark systems.
- Multi-factor authentication (MFA) policies have been further enhanced.

ASSETMARK

We have noted your account(s) with internal fraud warnings as a safety precaution. If you so choose, we can also change your account number(s) by calling your Financial Advisor or AssetMark toll-free at 800-664-5345.

We are providing, at no cost to you, a two-year subscription to ID Shield, a credit monitoring service that will monitor and protect your credit data and alert you if your Social Security number, credit cards, and/or bank account numbers are found in unsecure online locations. You will find more information about the services ID Shield offers following this letter.

In order to receive this free credit monitoring service, you will need to complete the enrollment process described in an email that you will receive directly from ID Shield. For security reasons, we are unable to complete this step of the process for you. Please let ID Shield know if you do not receive the enrollment email, by calling 800-654-7757.

What You Can Do

We have included a list of recommended steps to help protect your personal information in the enclosed materials.

For More Information

For more information or if you have any questions, please contact your Financial Advisor. Additionally, you may contact Jim Attaway, Senior Vice President, Infrastructure and Chief Information Security Officer, at jim.attaway@assetmark.com. You may also contact AssetMark toll-free at 800-664-5345.

Sincerely,

Claire Blue

Claire Blue
Chief Compliance Officer
AssetMark, Inc.
claire.blue@assetmark.com

Recommended Steps to Help Protect Your Information

1. Enroll in ID Shield Monitoring: We have arranged for you to enroll, for free, in a two-year subscription of ID Shield, a credit monitoring and identity theft protection service. ID Shield provides monitoring and protection and also alerts you of certain activities that could indicate potential identity theft.

Enrollment Procedure: To activate this coverage, please visit the website below using your member number that you receive via email.

1. CREATE your account at idshield.cloud/activate using your member number
2. ADD the personal information you want to monitor, including your social media accounts
3. DOWNLOAD the IDShield mobile app for immediate alerts and to track your monthly credit score.

If you are not able to enroll online, please call the toll-free number at 800-654-7757.

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel.

2. Monitor your Account(s) and Notify Us of Suspicious Activity: We recommend that you carefully monitor your account(s) for incidents of fraud and identity theft over the next 12-24 months. If you discover any suspicious or unusual activity on your account(s) or suspected identity theft or fraud, report it immediately to us.

3. 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.

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.

4. 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	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.

5. 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 in writing 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. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

6. 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.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

Maryland Residents: Office of the Attorney General, Attn: Security Breach Notification, 200 St. Paul Place, Baltimore, MD 21202, Fax: Attn: Security Breach Notification (410) 576-6566, Email: Idtheft@oag.state.md.us, website: Maryland Attorney General - ID Theft.