

July 24, 2024

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of Accident Fund Insurance Company of America (“Accident Fund” or the “Company”) to notify you regarding the nature and circumstances of a recent data security issue.

On June 20, 2024, Accident Fund learned that an unauthorized third party gained access to some of the Company’s systems. Promptly after becoming aware of the issue, the Company began to investigate its nature and scope with the assistance of external cybersecurity experts. In the course of its investigation, the Company determined on July 2, 2024, that the unauthorized party gained access to certain Company directory data on June 20, 2024. The affected information included employee names, work telephone numbers, work email addresses, work locations (field or office location), and Company system credentials (usernames and passwords).

After learning of the incident, Accident Fund quickly took steps to block the unauthorized party’s access to Company systems, including by disconnecting certain systems. The Company also reset all affected Company system passwords and is coordinating with law enforcement authorities. Accident Fund also has put in place additional monitoring measures to further protect its systems.

There are approximately 7 Maryland residents affected by this issue. Enclosed for your reference is a copy of the notice that will be sent via email to the affected Company employees.

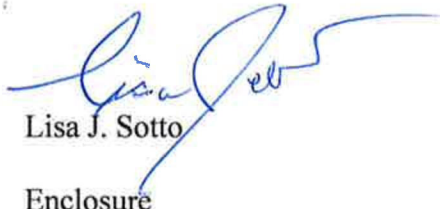
Office of the Attorney General

July 24, 2024

Page 2

Please do not hesitate to contact me if you have any questions.

Very truly yours,



Lisa J. Sotto

Enclosure

Notice of Data Breach



7/24/24

Dear Name,

As noted in yesterday's email, this message provides formal notification and details related to AF Group's recent cyber security incident.

What Happened?

On June 20, 2024, we learned that an unauthorized third party gained access to some of our systems. Promptly after becoming aware of the issue, we began to investigate its nature and scope. In the course of our investigation, we determined on July 2, 2024, that the unauthorized party gained access to certain company directory data on June 20, 2024.

What Information Was Involved?

The affected information included your name, work telephone number, work e-mail address, work location (field or office location) and company system credentials (username and password).

What We Are Doing

After learning of the incident, we quickly launched an investigation with the assistance of external cybersecurity experts and took steps to block the unauthorized party's access to our systems, including by disconnecting certain systems. We also reset all affected system

passwords and are coordinating with law enforcement authorities. We take the security of our data and systems very seriously and have put in place additional monitoring measures to further protect our systems.

What You Can Do

We recommend you change your password for any other online account on which you used a password that is the same as or similar to your company system password. We also recommend that you be cautious of any unsolicited communications involving your personal information and avoid clicking on links or downloading attachments from suspicious communications. The Reference Guide below provides additional recommendations by the U.S. Federal Trade Commission on the protection of personal information.

For More Information

We regret any inconvenience this issue may cause. If you have questions or need assistance, please contact compliance@afgroup.com.

Sincerely,

Kevin Zielke
Senior Vice President, General Counsel and Compliance Officer

U.S. Reference Guide

We encourage you to take the following steps:

Report Incidents. If you are in the U.S. and detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Additional Information. If you would like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three major nationwide credit reporting agencies. To protect yourself from possible identity theft, you may also consider placing a fraud alert or security freeze on your credit file. You can place a fraud alert on

your credit report by calling any one of the toll-free numbers provided below. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on fraud alerts and security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

Equifax
Equifax Information
Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285
www.equifax.com

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

TransUnion
TransUnion LLC
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
(800) 771-7755 (toll-free)
(800) 788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>

For Oregon Residents. You are encouraged to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.



The information contained in this communication is highly confidential and is intended solely for the use of the individual(s) to whom this communication is directed. If you are not the intended recipient, you are hereby notified that any viewing, copying, disclosure or distribution of this information is prohibited. Please notify the sender, by electronic mail or telephone, of any unintended receipt and delete the original message without making any copies.