



American International Group, Inc.
28 Liberty Street, 49th Floor
New York, NY 10005-1445

T (+1) 212.458.9153
C (+1) 973.487.6266
conrad.naas@aig.com
www.aig.com

February 23, 2023

BY EMAIL

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
IDtheft@oag.state.md.us

Re: Notice of Cybersecurity Incident

To Whom It May Concern:

Pursuant to Md. Code Ann., Com. Law § 14-3504, AIG Claims, Inc. ("AIG Claims") provides notice of a cybersecurity incident that occurred at AIG Claims' vendor, Elevate Services, Inc. ("Elevate"), between March 5, 2022, and March 15, 2022 (the "Elevate Security Incident" or the "Incident"). To be clear, there has been no impact to AIG Claims' operations or systems as a result of this Incident. AIG Claims is a subsidiary member of American International Group, Inc., a global insurance organization, and provides claims administration services for claims made against the insureds of its insurance company affiliates. Elevate provided AIG Claims with specialized administration services relating to the evaluation of certain claims. Elevate's principal place of business is 2375 E. Camelback Road, Suite 690, Phoenix, AZ 85016.

AIG Claims has determined that a number of individuals whose claims were administered by AIG Claims were among those identified by Elevate as among those whose data was affected in the Elevate Security Incident. We confirmed on January 25, 2023 that that data included one individual residing in Maryland. The types of personal information exposed included: name, medical information, and health insurance information. According to Elevate, while it was able to determine which servers the threat actors had access to, it was not able to, in all cases, identify whether such data was, in fact, accessed or exfiltrated by the threat actors. Accordingly, AIG Claims is treating all data as though it were exfiltrated.

AIG Claims first became aware of the Elevate Security Incident on December 5, 2022, via a phone call from Elevate. At the time, it was not clear what data from AIG Claims, if any, were involved. According to Elevate, it had previously attempted to notify AIG Claims about the Incident in November 2022, after completing its review of the affected data files to attribute them to clients, but AIG Claims has no record of receiving that notice. During the December 5th call, and in subsequent exchanges, Elevate informed AIG Claims that, while it had identified certain individuals purportedly associated with data belonging to AIG Claims, it had not ascertained the specific data elements contained in those data nor had it verified states of residency for any of those individuals.

On December 22, 2022, at AIG Claims' request, Elevate shared the affected data files purportedly associated with AIG Claims. AIG Claims began its review that same day to evaluate its data breach notification obligations. On December 23, 2022, AIG Claims confirmed that data, including PII, belonging to its insureds' claimants were included in the affected dataset, and matched that data to the affected individuals' states of residency. AIG Claims completed its review on



January 25, 2023, confirming that only one individual's information was involved. Based on this information, AIG Claims determined that it would be required to notify your office about this Incident.

Elevate has represented to AIG Claims that it engaged third-party vendors to respond to the incident and that one of these vendors concluded on June 7, 2022, that there were no lingering threats to Elevate's systems. Elevate has also reported that it has hardened its IT security and deployed continuous monitoring technology on its endpoints. Notice to individuals was not delayed as a result of a law enforcement investigation. To date, AIG Claims has received no reports of identity theft or fraud from affected individuals. AIG Claims understands that it is one of many Elevate customers impacted by the Incident and does not appear to have been targeted specifically.

Although AIG Claims' systems were not impacted by Elevate's Security Incident, AIG Claims is assessing whether any of its policies, procedures, or training would benefit from any enhancements in light of the Elevate Security Incident.

AIG Claims takes the protection of personal information very seriously and is committed to answering any questions your office may have. Please do not hesitate to contact me at Conrad.Naas@AIG.com or (212) 458-9153.

Respectfully yours,

A handwritten signature in black ink, appearing to read "Conrad J. Naas", written in a cursive style.

Conrad J. Naas
Senior Vice President and Deputy General Counsel
AIG Claims, Inc.

[Enclosure]



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

On behalf of AIG Claims, Inc., Elevate Services, Inc. ("Elevate" or "we") is writing to inform you of a recent data security event that occurred at Elevate that may involve some of your personal information. Elevate acts as a third-party service provider to AIG Claims, Inc. to carry out insurance claims administration services. Both Elevate and AIG Claims, Inc. take the protection of your personal information very seriously and deeply regret that this incident occurred. Although we are unaware of any cases of identity theft as a result of this incident, we are providing you with information about the event, Elevate's response, and steps you may take to better protect against the possibility of identity theft and fraud.

What Happened? On March 14, 2022, we became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption, including some we used to store data on behalf of AIG Claims, Inc. We immediately took steps to secure our systems and launched an investigation to determine the full nature and scope of the event. We also promptly notified federal law enforcement. Through our investigation, we determined that a malicious actor gained access to a limited number of our systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the malicious actor.

We performed a review of the contents of the affected systems to determine what information could have been contained in the impacted files and to whom the information related. Upon completion of the review, we then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and the Elevate customers, including AIG Claims, Inc., with whom they were associated.

What Information Was Involved? The scope of your personal information that was affected includes the following types of information relating to you: <<b2b_text_3(data elements)>>.

What We Are Doing. We take this event and the security of your information very seriously. Upon becoming aware of the event, we immediately took steps to secure our systems. We also conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. This notification was not delayed due to any law enforcement investigation. Additionally, while we have safeguards in place to protect data in our care, we further enhanced our technical and administrative processes as part of our ongoing commitment to data security. As an additional precaution, we are offering complimentary credit monitoring and identity restoration services for twelve (12) months through Kroll. For enrollment instructions, see below under "Steps You Can Take to Protect Personal Information."

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed "Steps You Can Take to Protect Personal Information." There you will find more information on the credit monitoring and identity restoration services we are making available to you. While we will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (855) 624-3241, Monday through Friday, 9:00 am to 6:30 pm Eastern Standard Time (except U.S. holidays). You may also write to Elevate at 2375 E. Camelback Road, Suite 690, Phoenix, AZ 85016.

Sincerely,

A handwritten signature in black ink, appearing to read "Steve Harmon", with a long horizontal flourish extending to the right.

Steve Harmon
Chief Operating Officer & General Counsel
Elevate Services, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL

INFORMATION Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<MembershipNumber(S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses 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 (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission ("FTC") may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

For Arkansas, California, Colorado, Florida, Illinois, Iowa, Kansas, Missouri, Nevada, Ohio, South Carolina, Texas, Virginia residents, you may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s). You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit

and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are # Rhode Island residents impacted by this event.