WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

November 24, 2020

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via First Class Mail

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident
Client: USG Insurance Services, Inc.
File No.: 16428.00003

Dear Attorney General MacDonald:

We represent USG Insurance Services, Inc. ("USG") an insurance company with multiple locations throughout the country. USG is headquartered in Canonsburg, Pennsylvania. USG takes the security and privacy of the information in its control seriously, and is taking steps to prevent a similar incident from reoccurring in the future.

1. **Nature of the incident.**

On October 27, 2020 USG discovered that an unauthorized user had gained access to its network. Upon discovery of the unauthorized access, USG immediately engaged a third party professional cybersecurity forensics team to investigate the incident and determine the scope and extent of the unauthorized access and determine whether any sensitive USG employee information was compromised. The forensics investigation discovered that the unauthorized individual may have had access to USG's server that stores employee Personally Identifiable Information ("PII"). The data potentially accessed includes individual's first and last name in combination with one or more of the following attributes: address, date of birth, driver's license and/or state identification number, passport number, Social Security number and / or financial information.

2. **Number of New Hampshire residents affected.**

Five (5) New Hampshire residents were potentially affected by this incident. Incident notification letters addressed to those individuals will be mailed on November 25, 2020, via First Class Mail. A sample copy of the Incident notification letter being mailed to potentially affected residents of New Hampshire is included with this letter at **Exhibit A**.

3. **Steps taken.**

At this time, there is no evidence that any employee information has been misused as a result of this incident. USG takes the security of all the information in its control very seriously, and is taking steps to prevent a similar event from occurring in the future, including but not limited to implementing tenant wide password changes and updating and installing enhanced security measures such as Carbon Black. Carbon Black is a software that is designed to detect malicious behavior and helps prevent malicious files from attacking an organization.

USG has also provided the affected individuals with complimentary credit monitoring services for a period of twelve (12) months.

4. Contact information.

USG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

EXHIBIT A

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident involving USG Insurance Services, Inc. ("USG") that may have resulted in the unauthorized access to some of your personal information. USG takes the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to help protect your information.

On October 27, 2020 USG discovered that an unauthorized user had gained access to its network. Upon discovery of the unauthorized access, USG immediately engaged a third-party professional cybersecurity forensics team to investigate the incident and determine the scope and extent of the unauthorized access and determine whether any sensitive USG employee information was compromised.

The forensics investigation discovered that the unauthorized individual may have had access to some of your employee data and Personally Identifiable Information ("PII"). The data potentially accessed includes your first and last name in combination with one or more of the following attributes: address, date of birth, driver's license and/or state identification number, passport number, Social Security number and financial information.

At this time, there is no evidence that any employee information has been misused as a result of this incident. However, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring services, at no cost to you, for twelve months.

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, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **February 28, 2021** to activate your identity monitoring services.*
Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

We take the security of all information in our control very seriously, and are taking steps to help prevent a similar event from occurring in the future, including but not limited to updating and installing enhanced security measures and implementing tenant wide password changes.

We sincerely regret any inconvenience that this matter may cause you and remain dedicated to maintaining the security and protection of your information. We encourage you to remain vigilant and review the enclosed addendum outlining additional steps you can take to help protect your personal information. If you have any questions or want to enroll in the complimentary identify monitoring services, please call 1-???-???-???? Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Timothy Horton
President

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618 www.illinoisattorneygeneral.gov

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Kroll | A Division of DUFF&PHELPS

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 will 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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to 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.