Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 1, 2024

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, IA 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent TRISTAR Insurance Group ("TRISTAR") located at 100 Oceangate #840, Long Beach, CA 90802, and are writing to notify your office of an incident that may affect the security of certain personal information relating to six thousand sixty-nine (6,069) Iowa residents. TRISTAR is a third-party insurance claims administrator, managing claims for several alternatively funded entities in both the private and public insurance segments. TRISTAR is providing this notification on behalf of itself and its customers, as those customers' data was stored on TRISTAR systems impacted by the event. The vast majority of the above referenced impacted Iowa residents are affiliated with TRISTAR's customers.

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TRISTAR does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

Over one year ago, or about November 10, 2022, TRISTAR became aware of suspicious activity on certain computer systems. TRISTAR immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. TRISTAR's investigation determined that there was unauthorized access to their email environment beginning on November 4, 2022, and that the unauthorized actor was ultimately able to gain access to certain TRISTAR systems beginning on November 9, 2022. Through the investigation, TRISTAR learned that certain information related to its customers was stolen from TRISTAR's network. TRISTAR therefore undertook a comprehensive and time intensive review of potentially impacted files, with the assistance of

third-party subject matter specialists, to determine the names and contact information of individuals whose information was contained in the potentially impacted files. TRISTAR has seen no evidence of misuse of any information impacted in this event. Additionally, there is no evidence that TRISTAR's claims or accounting systems were breached during this incident.

The information that could have been subject to unauthorized access includes name, financial account information, Social Security number, and Government identification number.

Notice to Iowa Residents

On or about February 1, 2024, TRISTAR began providing written notice of this incident to approximately six thousand sixty-nine (6,069) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, TRISTAR moved quickly to investigate and respond to the incident, assess the security of TRISTAR systems, and identify potentially affected individuals. Further, TRISTAR notified federal law enforcement regarding the event. TRISTAR is also working to implement additional safeguards and training to its employees. TRISTAR is providing access to credit monitoring services for one (1) year through Epiq to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TRISTAR is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TRISTAR is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

TRISTAR is providing written notice of this incident to relevant state regulators, as necessary, as well as the three major credit reporting agencies (Experian, Equifax, and TransUnion).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/jrm
Enclosure

EXHIBIT A

TRISTAR
Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<First Name>> <<Last Name>>
<<Business or Representative Name>>
<<Address 1>>
<<Address 2>>
<<City>> <<State>> <<Zip>>

<<Date>>

Notice of Data <<Event/Breach>>

Dear <<First Name>> <<Last Name>>:

TRISTAR Insurance Group ("TRISTAR") writes to notify you of an event that may have affected the privacy of some of your information. TRISTAR is a third-party insurance claims administrator, managing claims for several alternatively funded entities in both the private and public insurance segments. TRISTAR provides services to various entities in the insurance industry, including <<Data Owner>>. To perform these services, TRISTAR was provided certain information by <<Data Owner>> which was present in its systems at the time of the event discussed in this letter. This letter includes details of the event, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? On or about November 10, 2022, TRISTAR became aware of suspicious activity on certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to our email environment beginning on November 4, 2022, and that the unauthorized actor was ultimately able to gain access to certain TRISTAR systems beginning on November 9, 2022. Through our investigation, we learned that certain information related to our customers was potentially exfiltrated from TRISTAR's network. TRISTAR therefore undertook a comprehensive and time intensive review of potentially impacted files, with the assistance of third-party subject matter specialists, and later determined that the files contained certain information related to you. TRISTAR has seen no evidence of misuse of any information related to this event. Additionally, there is no evidence that TRISTAR or <<Data Owner>>'s claims or accounting systems were breached during this incident.

What Information Was Involved? TRISTAR determined that the following information related to you was present within the impacted files: your name, <<Breached Elements>>.

What We Are Doing. Upon discovery, we immediately secured the environment and commenced an investigation to confirm the nature and scope of the event. We reported this event to law enforcement and are cooperating and assisting in their investigation. We also implemented additional technical safeguards, and reviewed policies and procedures relating to data privacy and security.

As an added precaution, we are also offering you complimentary access to <<12/24>> months of credit monitoring and identity theft restoration services, through Epiq. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Personal Information* for additional detail on these services.

What You Can Do. TRISTAR encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* for additional details on how to take steps to protect your information, should you feel it is necessary to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call 888-983-0350, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time. Additionally, you can write to us at TRISTAR Insurance Group, Attention: Incident Response, 100 Oceangate #840, Long Beach, CA 90802.

We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Tim McIntyre
General Counsel
TRISTAR Insurance Group

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Credit Monitoring

<<First Name>> <<Last Name>>
Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 1-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 credit 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 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 that in order 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 Massachusetts Residents, Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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 incident. There are <<RI Count>> Rhode Island residents impacted.