Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

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

March 25, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Horizon Actuarial Services, LLC ("Horizon Actuarial") located at 1040 Crown Pointe Pkwy, Suite 560, Atlanta, GA 30338, and are writing to notify your office on behalf of the entities listed in ***Exhibit A*** of an incident that may affect the security of some personal information relating to a total of three hundred nineteen (319) Iowa residents. The investigation into this matter is ongoing, and this notice will be supplemented as Horizon Actuarial receives requests from additional entities to provide notice on their behalf. By providing this notice, Horizon Actuarial 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

Horizon Actuarial provides technical and actuarial consulting services for benefit plans in the United States. For business and compliance purposes, Horizon Actuarial received the information of individuals who are or were participants in or had contributions made on their behalf to the benefit plans and in some cases, other individuals that may have been beneficiaries.

On November 12, 2021, Horizon Actuarial received an email from a group claiming to have stolen copies of personal data from Horizon Actuarial's computer system. Horizon Actuarial immediately initiated efforts to secure its computer system and with the assistance of third-party computer specialists, launched an investigation into the legitimacy of the claims in the email. Horizon Actuarial notified the FBI and negotiated with and paid the group in exchange for an agreement that they would delete and not distribute or otherwise misuse the stolen information.

Horizon Actuarial's investigation revealed that two of its computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The group provided Horizon Actuarial with a list of information they claimed to have stolen. On January 9, 2022, Horizon Actuarial determined that information relating various benefit plans for which it provides technical and actuarial consulting services was located on the list of files provided by the group. On January 13, 2022, Horizon Actuarial began providing notice of this event to its clients and other entities whose information was located on the list and offered to provide notice on behalf of the clients.

The information that could have been subject to unauthorized access includes name, address, Social Security number, bank account number, health insurance plan information and date of birth of three hundred nineteen (319) Iowa residents.

Notice to Iowa Residents

Beginning on March 25, 2022, Horizon Actuarial provided written notice of this incident to affected individuals, which includes three hundred nineteen (319) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, Horizon Actuarial moved quickly to investigate and respond to the incident, assess the security of Horizon Actuarial systems, and notify potentially affected individuals. Horizon Actuarial is also evaluating and implementing additional safeguards and providing additional training for its employees. Horizon Actuarial is providing access to credit monitoring services and identity theft and fraud support services for 12 months, through Kroll, LLC, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Horizon Actuarial is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Horizon Actuarial 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/arf

EXHIBIT A

Fund Name	**Number of Impacted Iowa Residents**
Airconditioning and Refrigeration Industry Retirement Trust Fund	3
Airconditioning and Refrigeration Industry Health and Welfare Trust Fund	1
UA Local 198 Pension Fund	4
Twin Cities Bakery Drivers Health & Welfare Trust	46
Twin Cities Bakery Drivers Pension Plan	170
Intermountain Retail Food Industry Pension Trust Fund	26
Rocky Mountain UFCW Health Benefit Plan for Retired Employees	25
Rocky Mountain UFCW Retail and Meat Pension Plan	19
Intermountain Retail Store Employees Pension Trust	14
Southern California Rock Products Retirement Plan	2
The Southern California Plastering Institute Pension Trust Fund	9

EXHIBIT B

Horizon
Actuarial Services, LLC®

<<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 (Notice of Data Breach)>>

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

Horizon Actuarial Services, LLC (Horizon Actuarial) is writing to make you aware of a data privacy incident that may affect the privacy of some of your information. Horizon Actuarial provides technical and actuarial consulting services for benefit plans in the United States. You are receiving this letter because you or your family member are or were a participant in, or had contributions made on your behalf to, the following benefit plan(s): <<b2b_text_3 (Benefit Plan/Data Owner)>><<b2b_text_4 (Benefit Plan/Data Owner cont.)>> (collectively, the "Fund"). Information was provided to Horizon Actuarial for business and compliance reasons. This letter provides details of the incident, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so. If you have any questions about this notice, please contact us at the number listed below under "For more information." Do not call your Fund administrator.

What Happened? On November 12, 2021, Horizon Actuarial received an email from a group claiming to have stolen copies of personal data from its computer servers. Horizon Actuarial immediately initiated efforts to secure its computer servers and with the assistance of third-party computer specialists, launched an investigation into the legitimacy of the claims in the email. Horizon Actuarial also provided notice to the FBI. During the course of the investigation, Horizon Actuarial negotiated with and paid the group in exchange for an agreement that they would delete and not distribute or otherwise misuse the stolen information.

The investigation revealed that two Horizon Actuarial computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The group provided a list of information they claimed to have stolen. On January 9, 2022, we determined potentially sensitive information was located in one of these files. We provided notice of the event to the Fund beginning on January 13, 2022, and subsequently provided a list of affected individuals. Horizon Actuarial began mailing letters to individuals associated with benefit plans that authorized them to do so.

The Fund's computers were not affected by the security incident. Any benefits that may be due have not been, and will not be, impacted by the security incident.

What Information Was Involved? Our investigation determined that the following types of information related to you may have been impacted: <<b2b_text_2 (Impacted Data)>>.

What We Are Doing. Horizon Actuarial takes this incident and the security of information in its care very seriously. Horizon Actuarial is reviewing its existing security policies and has implemented additional measures to further protect against similar incidents moving forward.

We have arranged for you to activate, at no cost to you, identity monitoring services for 12 months provided by Kroll.

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, $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 (Activation Date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

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

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via Kroll's automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing Kroll's services is included with this letter.

What You Can Do. Horizon Actuarial encourages potentially impacted parties to activate the complimentary identity monitoring services and remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring notices from their plans, including any Explanation of Benefits, and free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Information*."

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 1-855-541-3574, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holidays, do not call your Fund Administrator. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Mark K. Lewis
COO/CFO

Horizon
Actuarial Services, LLC®

Steps You Can Take to Help Protect Your Information

ACTIVATE YOUR IDENTITY MONITORING

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.

$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 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 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 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, military identification, 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 fraud alert or 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
888-298-0045	888-397-3742	833-395-6938
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

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 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 a 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 approximately [#] Rhode Island residents impacted by this incident.