CARY KANE

A LIMITED LIABILITY PARTNERSHIP FOR THE PRACTICE OF LAW

March 24, 2022

VIA EMAIL
Attorney General John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: doj-cpb@doj.nh.gov

Re: Notice of Data Breach

Dear Attorney General Formella:

On behalf of the **Soft Drink & Brewery Workers Union Local 812 Retirement Fund** (the "Fund"), and pursuant to N.H. Rev. Stat. § 359-C:19 *et seq*., we are writing to notify you of a recent information security incident incurred by a vendor **Horizon Actuarial Services, LLC** ("Horizon") involving six New Hampshire residents.

Name and Address of Business and the Type of Business
The Fund is a multiemployer benefit plan that provides pension benefits to members of Local 812 of the International Brotherhood of Teamsters (the "Union") under collective bargaining agreements between the members' employers and the Union. The Fund also provides pension benefits to certain individuals who work for the Union, the Fund, and a related welfare fund under written agreements between those entities and the Fund's Board of Trustees. The Fund's office is located at 455 Northern Boulevard, Great Neck, New York 11021.

Horizon is a private company that provides actuarial and consulting services to multiemployer benefit plans across various industries. Horizon has been providing actuarial services in connection with negotiations between certain participating employers, the Union and the Fund to fully fund the benefits due to the Fund's participants. Horizon is located at 1040 Crown Pointe Pkwy, Suite 560, Atlanta, GA 30338.

Nature of the Incident
On January 13, 2022, the Fund learned that Horizon was subject to a cybersecurity attack dating back to November 12, 2021 that involved the compromise of Fund participant data. Based on information provided by Horizon, on November 12, 2021, Horizon received an email from a group

claiming to have stolen copies of personal data from its computer servers. Horizon 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 also provided notice to the FBI. During the course of the investigation, Horizon negotiated with and paid the group in exchange for an agreement that they would delete and not distribute or otherwise misuse the stolen information. Currently, neither Horizon nor the Fund are aware of any fraud or misuse of Fund participant data.

We understand that the investigation revealed that two Horizon 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. Horizon provided notice of the event to the Fund on January 13, 2022, and subsequently provided a list of affected individuals on or about January 20, 2022. The Fund worked expeditiously to include address information identifying relevant states of residents, and Horizon agreed to provide notice to affected individuals occurring on or about March 25, 2022.

Response to the Incident
Based on information provided by Horizon, after learning of the incident, Horizon promptly initiated efforts to secure its system upon discovery, notified the FBI, and initiated an investigation to determine the nature and scope of the incident. Since the incident, Horizon has (i) appointed a new Chief Information Security Officer; (ii) upgraded its Security Operations Center to include enhanced Management Detection and Response services; and (iii) established a rapid response capability to address new cybersecurity threats.

Upon notification, the Fund has worked closely with Horizon, through legal counsel, to determine the appropriate notification steps for affected individuals.

The New Hampshire residents were notified on or about March 25, 2022. A sample notification letter is attached

Identity Theft Protection
Horizon is providing affected individuals free one-year identity monitoring services through Kroll, a global leader in risk mitigation and response. This identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. None of the notified individuals have been asked or required to waive any right of private action as a condition of accepting the credit monitoring services.

Contact Information
If you have any questions concerning this matter, please contact me on behalf of the Fund at (212) 871-0540, or sbruno@carykane.com.

Very truly yours,

Susan Bruno

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

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

Notice of Data Incident

Dear ***<< (Name)>>*** ,

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): Soft Drink & Brewery Workers' Union, Local 812 Retirement Fund (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: Social Security Number, Name, and Date of Birth

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

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

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 [Call Center TFN], 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

Steps You Can Take to Help Protect Your Information

ACTIVATE 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, you can obtain information from the Federal Trade Commission and the Office of the District of Columbia Attorney General about steps to take to avoid identity theft. You can contact the D.C. Attorney General: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Iowa Residents, state law advises to you to report any suspected identity theft to law enforcement or the Attorney General.

For Maryland residents, you can obtain information from the Maryland Attorney General about steps that you can take to help prevent identity theft: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For Massachusetts residents, you have a right to request from us a copy of any police report filed in connection with 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. As noted above, you also have the right to place a security freeze on your credit report at no charge.

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, you may contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office Bureau of Internet and Technology (212) 416-8433 https://ag.ny.gov/internet/resource-center	NYS Department of State's Division of Consumer Protection (800) 697-1220 https://www.dos.ny.gov/consumerprotection

For North Carolina residents, you can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

For Oregon residents, state laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

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 information about steps you can take to help prevent identity theft and a copy of any police report filed in regard to this incident. There are approximately [#] Rhode Island residents impacted by this incident.