Morgan Lewis

Ezra D. Church
Partner
+1.215.963.5710
ezra.church@morganlewis.com

March 22, 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 **Major League Baseball Players Benefit Plan** (the "Plan"), pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.*, we are writing to notify you of an information security incident from its vendor **Horizon Actuarial Services, LLC** ("Horizon") involving 39 New Hampshire residents.

Name and Address of Business and the Type of Business
The Plan provides pension and health benefits, to current and former players in Major League Baseball. The Plan is located at P.O. Box 1096, Sparks, MD 21152.

Horizon is a private company that provides actuarial and consulting services to multiemployer benefit plans across various industries, including the Plan. Horizon is located at 1040 Crown Pointe Pkwy, Suite 560 Atlanta, GA 30338.

Nature of the Incident
On January 13, 2022, the Plan learned that Horizon experienced a cybersecurity attack dating back to November 12, 2021. According to information provided by Horizon, Horizon received an email on November 12, 2021, from a group claiming to have stolen copies of personal data from its computer servers. Horizon 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 Plan are aware of any fraud or misuse of 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. Notice regarding the compromise of personal information was provided to the Plan on January 13, 2022, and Horizon subsequently provided a list of affected individuals on or about January 28, 2022. The Plan worked expeditiously to include address information identifying relevant states of residence, and Horizon agreed to provide notice to participants to occur on or about March 22, 2022.

What Information was Involved?
After Horizon's investigation, it determined that the personal information accessed included name, address, telephone number, date of birth, social security number, and certain benefits information.

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.

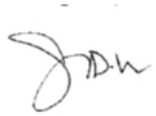
Upon notification, the Plan worked closely with Horizon, through legal counsel, to determine the appropriate notification steps for affected individuals.

The New Hampshire residents were notified on or about March 22, 2022. A sample notification letter is attached.

Identity Theft Protection
Horizon is providing a complimentary 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 Plan at (215) 963-5710, or ezra.church@morganlewis.com.

Best regards,



Ezra D. Church

Enclosure
Sample Individual Notification Letter

Horizon Actuarial Services, LLC®

Para hablar con un agente de habla hispana sobre este aviso y los servicios ofrecidos, o para recibir una copia impresa en español, llame al 1-855-541-3574.

<<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 an 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 Major League Baseball Players Benefit Plan, through which your information was provided to Horizon Actuarial for business and compliance purposes. 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.

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

Our investigation revealed that two of our computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The unauthorized group provided us with a list of information they claimed to have stolen. We are notifying all individuals whose information was located in the files for your benefit plan(s). On January 9, 2022, we determined potentially sensitive information related to your plan was located in one of these files, and we provided notice of the event to your health and/or pensions plan(s) on January 13, 2022, and subsequently provided a list of affected individuals.

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)>>. Information about your individual health claims was not accessed.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon discovering this incident, we immediately took steps to review and reinforce the security of our systems. We are reviewing our existing security policies and have implemented additional measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information.

In addition, we have arranged for you to activate, at no cost to you, an online credit monitoring service 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 our 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 your services is included with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring notices from your plan, 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. 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 YOUR CREDIT AND 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'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.

$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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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; 1-410-528-8662 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 https://files.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.

Horizon Actuarial Services, LLC®

Para hablar con un agente de habla hispana sobre este aviso y los servicios ofrecidos, o para recibir una copia impresa en español, llame al 1-855-541-3574.

<<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 an 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 Major League Baseball Players Benefit Plan, through which your information was provided to Horizon Actuarial for business and compliance purposes. 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.

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

Our investigation revealed that two of our computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The unauthorized group provided us with a list of information they claimed to have stolen. We are notifying all individuals whose information was located in the files for your benefit plan(s). On January 9, 2022, we determined potentially sensitive information related to your plan was located in one of these files, and we provided notice of the event to your health and/or pensions plan(s) on January 13, 2022, and subsequently provided a list of affected individuals.

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)>>. Information about your individual health claims was not accessed.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon discovering this incident, we immediately took steps to review and reinforce the security of our systems. We are reviewing our existing security policies and have implemented additional measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information.

In addition, we have arranged for you to activate, at no cost to you, an online credit monitoring service for 24 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 our 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 your services is included with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring notices from your plan, 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. 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 YOUR CREDIT AND 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'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.

$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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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; 1-410-528-8662 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 https://files.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.

Horizon Actuarial Services, LLC®

Para hablar con un agente de habla hispana sobre este aviso y los servicios ofrecidos, o para recibir una copia impresa en español, llame al 1-855-541-3574.

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

Next of Kin of
<<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 Next of Kin of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Horizon Actuarial Services, LLC (Horizon Actuarial) is writing to make you aware of an incident that may affect the privacy of some of your loved one's information. Horizon Actuarial provides technical and actuarial consulting services for benefit plans in the United States. You are receiving this letter because your loved one was a participant in, or had contributions made on their behalf to, the Major League Baseball Players Benefit Plan, through which your loved one's information was provided to Horizon Actuarial for business and compliance purposes. 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.

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

Our investigation revealed that two of our computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The unauthorized group provided us with a list of information they claimed to have stolen. We are notifying all individuals whose information was located in the files for your benefit plan(s). On January 9, 2022, we determined potentially sensitive information related to the plan was located in one of these files, and we provided notice of the event to the health and/or pensions plan(s) on January 13, 2022, and subsequently provided a list of affected individuals.

What Information Was Involved. Our investigation determined that the following types of information related to your loved one may have been impacted: <<b2b_text_2 (Impacted Data)>>. Information about your individual health claims was not accessed.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon discovering this incident, we immediately took steps to review and reinforce the security of our systems. We are reviewing our existing security policies and have implemented additional measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to protect your loved one's information.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your loved one's account statements and monitoring notices from their plan, 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 Loved One's 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. 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 LOVED ONE'S INFORMATION

MONITOR ACCOUNTS

We encourage you to monitor your loved one's account statements, and to monitor your loved one's credit reports for suspicious activity. In addition, there are steps you can take to protect your loved one's credit file. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. To order this free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

You may also request, in writing, that the report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

Contact information for the three major credit bureaus is 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	1-833-395-6938
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; 1-410-528-8662 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 https://files.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.

Horizon
Actuarial Services, LLC®

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

Parent or Guardian of
<<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 Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Horizon Actuarial Services, LLC (Horizon Actuarial) is writing to make your minor child aware of an incident that may affect the privacy of some of their information. Horizon Actuarial provides technical and actuarial consulting services for benefit plans in the United States. Your minor child is receiving this letter because they are or were a participant in, or had contributions made on their behalf to, the Major League Baseball Players Benefit Plan, through which their information was provided to Horizon Actuarial for business and compliance purposes. This letter provides details of the incident, our response, and resources available to you to help protect your minor child's information, should you feel it is appropriate to do so.

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

Our investigation revealed that two of our computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The unauthorized group provided us with a list of information they claimed to have stolen. We are notifying all individuals whose information was located in the files for your benefit plan(s). On January 9, 2022, we determined potentially sensitive information related to the plan was located in one of these files, and we provided notice of the event to the health and/or pensions plan(s) on January 13, 2022, and subsequently provided a list of affected individuals.

What Information Was Involved. Our investigation determined that the following types of information related to your minor child may have been impacted: <<b2b_text_2 (Impacted Date)>>. Information about their individual health claims was not accessed.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon discovering this incident, we immediately took steps to review and reinforce the security of our systems. We are reviewing our existing security policies and have implemented additional measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including your minor child, so that you may take steps to protect their information.

What You Can Do. We encourage you to 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 or your minor child may have questions about this incident that are not addressed in this letter. If you or your minor child 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. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you or your minor child.

Sincerely,

Mark K. Lewis
COO/CFO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR MINOR CHILD'S INFORMATION

MONITOR YOUR MINOR CHILD'S ACCOUNTS

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your minor child's account statements for suspicious activity. Typically, a minor child under the age of eighteen (18) does not have credit in his or her name, and the consumer reporting agencies do not have a credit report in a minor child's name. To find out if your minor child has a credit report or to request a manual search for your minor child's Social Security number each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit the below websites:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/form-minor-child.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-disputes/child-identity-theft-inquiry-form

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
https://www.equifax.com/personal/help/request-child-credit-report/

Adults and minors, sixteen (16) years or older, have the right to place a "security freeze" on a credit report, which will prohibit a consumer reporting agency from releasing information in the credit report without express authorization. A parent or guardian also has the right to place a "security freeze" on a minor's credit report if the child is under the age of sixteen (16). This right includes proactively placing a "security freeze" on a minor's credit report if the minor is under sixteen (16) years old. If the nationwide credit reporting agencies don't have a credit file on the minor, they will create one so they can freeze it. This record can't be used for credit purposes. It's there to make sure the child's record is frozen and protected against potential identity theft and fraud. Pursuant to federal law, you cannot be charged to place or lift a security freeze on a credit report. Should you wish to place a security freeze on a credit file or proactively place a freeze on a minor's credit report, please contact the major consumer reporting agencies 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	1-833-395-6938
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

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 above.

To request information about the existence of a credit file in your minor child's name, search for your minor's Social Security number, place a security freeze on your minor's credit file, place a fraud alert on your minor's credit report (if one exists), or request a copy of your minor's credit report you may be required to provide the following information:

1. A copy of your driver's license or another government issued identification card, such as a state ID card, etc.;
2. Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
3. A copy of your minor's birth certificate;
4. A copy of your minor's Social Security card;
5. Your minor's full name, including middle initial and generation, such as JR, SR, II, III, etc.; and
6. Your minor's date of birth; and previous addresses for the past two years.

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.

Additional Information

You may further educate yourself and your minor child 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; 1-410-528-8662 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 https://files.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.