POLSINELLI

150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

August 2, 2019

Bruce A. Radke
312-463-6211
312-819-1910
bradke@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent National Baseball Hall of Fame and Museum ("Hall of Fame") in connection with an incident that involved the personal information of forty-two (42) New Hampshire residents and provide this notice on behalf of the Hall of Fame pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While the Hall of Fame is notifying you of this incident, the Hall of Fame does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

The Hall of Fame recently learned that an unauthorized third party injected malicious code into the Hall of Fame's Web Store. The code was removed as soon as it was discovered but could have been able to collect information that customers entered on the Web Store's check-out page while it was active on the Web Store. That information included customers' names, addresses, and credit or debit card information, including CVV codes and expiration dates. The incident did not impact any Social Security numbers or driver's license information. The Hall of Fame is notifying individuals who made credit card purchases via the Web Store between November 15, 2018 and May 14, 2019.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On June 18, 2019, the Hall of Fame determined that forty-two (42) New Hampshire residents may have been impacted by this incident. The Hall of Fame is notifying impacted residents of the situation by letter today, August 2, 2019. Enclosed is a copy of the notice that is being sent to the impacted residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, the Hall of Fame promptly retained a forensic security firm to investigate the incident and notified law enforcement. The Hall of Fame also removed the malicious code from its Web Store. Additionally, the Hall of Fame has taken steps to alert the credit card brands of the incident so they can monitor the affected individuals' accounts for potential fraudulent activity. Finally, the Hall of Fame has taken additional technical steps to further secure its Web Store and prevent this type of incident from occurring in the future.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Bruce A. Radke

Enclosure

cc: Jeff Jones, SVP Finance & Administration, National Baseball Hall of Fame and Museum

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

The National Baseball Hall of Fame ("Hall of Fame") values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. On June 18, 2019, we learned that some of your information could have been obtained by an unauthorized third-party that placed malicious computer code on the Hall of Fame web store (shop.baseballhall.org) e-commerce system. The code may have targeted certain personal information of customers who made a credit card purchase via the web store between November 15, 2018 and May 14, 2019.

We are notifying you about the incident because we determined that you entered some personal information on the checkout page during the time the malicious code was active on our web store. This information included your name, address and your credit or debit card information, including your CVV code. The incident did not impact your Social Security Number or driver's license information.

Upon learning of the incident, we promptly retained a forensic security firm to investigate the incident and have notified law enforcement. We also removed the malicious code from our web store. Additionally, we have taken steps to alert the credit card brands of the incident so they can monitor your account for potential fraudulent activity. Finally, we have taken additional technical steps to further secure our web store and prevent this type of incident from occurring in the future.

We value the trust you place in us to protect your privacy, take our responsibility to safeguard personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 1-???-???-???? from 9:00 a.m. to 6:30 p.m. ET, Monday through Friday.

Sincerely,

Sean J. Gahagan
Vice President, Retail Merchandising and Licensing
National Baseball Hall of Fame and Museum

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 1 year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To remove the security freeze or lift the freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove or lift the security freeze for those identified entities or for the specified period of time.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

For residents of Iowa: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

For residents of Maryland: Maryland residents can contact the Office of the Attorney General to obtain information about steps one can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us

For residents of Rhode Island: We believe that this incident affected forty-two (42) Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. An individual has the right to obtain any police report filed in regard to this incident. If one is the victim of identity theft, they also have the right to file a police report and obtain a copy of it.

For residents of North Carolina: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.