EXHIBIT 1

By providing this notice, National Intramural and Recreational Sports Association ("NIRSA") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 26, 2020, NIRSA became aware of suspicious activity on its system. Immediately thereafter, NIRSA began working with a third-party computer forensic firm to determine the event timeline and threat posed to any sensitive data stored on NIRSA's system. On July 28, 2020, the investigation confirmed that the contents of NIRSA's database were accessible to unknown individual(s). We note, however, there is no direct evidence that the database contents were actually accessed or acquired by the unauthorized individual(s).

NIRSA then undertook a lengthy and time-consuming review of the contents of the database to accurately determine the information relating to its members that would be considered at risk. Once this review was complete, NIRSA took steps to notify individuals.

The information relating to potentially impacted individuals includes name, address and a combination of username, password, and/or date of birth.

Notice to Maine Residents

On October 23, 2020, NIRSA provided written notice of this incident to potentially affected individuals, which includes fifteen (15) Maine residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, NIRSA moved quickly to investigate and respond to the incident, assess the security of NIRSA systems, and notify potentially affected individuals. NIRSA is also working to implement additional safeguards and training to its employees.

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

EXHIBIT A

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Re: Notice of Data Breach>>

Dear <<Name 1>>,

National Intramural and Recreational Sports Association ("NIRSA") is writing to notify you of an incident that may affect the security of certain personal information. NIRSA takes this incident very seriously and is providing you with details about the incident, our response, and steps you can take to better protect your payment card information, should you feel it appropriate to do so.

What Happened? On May 26, 2020, NIRSA became aware of suspicious activity on its system. Immediately thereafter, NIRSA engaged a third-party computer forensic firm to determine the event timeline and threat posed to any sensitive data stored on NIRSA's system. On July 28, 2020, the investigation confirmed that the contents of NIRSA's database were accessible to unknown individual(s). We note, however, there is no direct evidence that the database contents were actually accessed or acquired by the unauthorized individual(s). We are simply notifying you out of an abundance of caution.

NIRSA then undertook a lengthy and time-consuming review of the contents of the database to accurately determine the information relating to its members that would be considered at risk. Once this review was complete, NIRSA took steps to notify you.

What Information Was Involved? NIRSA's investigation into the incident determined your name, address and a combination of your e-mail, username, password, and/or date of birth may have been compromised.

What NIRSA is Doing. NIRSA takes the security of your personal information seriously. We immediately retained a forensic investigation firm to determine the nature and scope of this incident. We are also working to improve security protocols already in place to continue to protect against potential unauthorized activity.

What You Can Do. While there is no evidence that your credentials (or any other information) were compromised, we encourage you to promptly change the password on the NIRSA site and change any other passwords that are the same or similar. It is best practice to have complex and unique passwords for each separate account. Please also refer to the enclosed *Steps You Can Take to Protect Personal Information* for additional guidance.

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 the dedicated assistance line that we have helped set up at 888-490-0596, Monday through Friday from 9 a.m. to 9 p.m., excluding U.S. holidays.

We sincerely regret any inconvenience this incident may cause you and we remain committed to safeguarding your information within our care.

Sincerely,

National Intramural and Recreational Sports Association

Steps You Can Take to Protect Personal Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of payment card fraud or misuse, to review your account statements, and to monitor your credit reports for suspicious activity. If you see any unauthorized or suspicious activity, promptly contact your bank, credit union, or credit card company.

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your 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 credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will 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.

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 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 agencies listed below:

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-alerts

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or the state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Ave. NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); or 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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **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 agencies 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. You can 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. NW, Washington, DC 20580. **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. **North Carolina Residents:** Office of the Attorney General of North Carolina**,** Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll-free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 49 Rhode Island residents impacted by this incident. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.