MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

September 13, 2019

VIA U.S. MAIL & E-MAIL

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
Email: ndag@nd.gov

Re: Notice of Data Security Event

Dear Sir or Madam:

We represent the Amateur Athletic Union ("AAU"), located at 1910 Hotel Plaza Blvd., Lake Buena Vista, Florida 32830. We are writing to notify your office of an incident that may affect the security of payment card information relating to five hundred ninety-five (595) North Dakota residents. The investigation into this matter is ongoing, and this notice may be supplemented if new significant facts are learned subsequent to its submission. By providing this notice, AAU does not waive any rights or defenses regarding the applicability of North Dakota law, the applicability of the North Dakota data event notification statute, or personal jurisdiction.

Nature of the Data Event

AAU, working with third party forensic investigators, identified signs of malicious code on the checkout page of its website, play.aausports.org, on August 2, 2019. The investigation determined that this code was capable of capturing certain information entered into the checkout page of AAU's website between October 1, 2018 and July 2, 2019. Upon making the determination of when the code was present on the website, AAU reviewed its transaction records to determine the identities of its members whose payment card information may be impacted. AAU recently confirmed the identities of the individuals whose payment card information may have been impacted and completed efforts to locate the address information for these individuals. The code at issue was removed from the site and members can safely use their payment card on AAU's website.

The information that could have been subject to unauthorized access includes cardholder name, address, credit card number, expiration date, and CVV.

192396

Notice to North Dakota Residents

On or about September 13, 2019, AAU began providing written notice of this incident to affected individuals, which includes five hundred ninety-five (595) North Dakota residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

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

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

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/plm
Enclosure

EXHIBIT A

Return Mail Processing Center
PO 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>>

Dear <<Name1>>:

The Amateur Athletic Union (AAU) is writing to inform you about a recent event that may have impacted the payment information for some website visitors and to assure you that we've taken additional steps to safeguard against future incidents. The AAU takes this incident and the security of your information very seriously.

The AAU has worked tirelessly during its 131 years of service to earn the public's trust as a champion of amateur sports across America, and we're committed to taking whatever steps necessary to maintain your ongoing support for that mission.

As a first step, we wanted to explain what happened and how we responded. We also want to tell you how to better protect yourself against potential fraud, if you think it's needed.

What Happened? On August 2, 2019, AAU, with the assistance of third-party forensic investigators, identified signs of malicious code on our site, play.aausports.org and determined that the code could capture information entered onto the site's checkout page from October 1, 2018 to July 2, 2019.

What Information Is Involved? The information potentially captured by the code includes the cardholder's name, address, and payment card information -- including number, expiration date, and CVV.

What We Are Doing. After determining exactly when the code was on the site, the AAU reviewed transaction records to promptly identify the names and addresses of everyone whose payment card data might have been compromised. We have completed that effort, and the code has been removed, which allows site visitors to again safely use their payment card on the checkout page.

With support from a team of forensics experts, we have conducted a thorough website review, in addition to implementing enhanced security measures to reduce the risk of a similar incident. The AAU has also notified the required state regulators and consumer reporting agencies about this incident. We want to again express our hope that these steps will help maintain your trust in the AAU as we move forward.

What You Can Do. You can learn more about how to protect against potential fraud in the enclosed "Steps You Can Take to Prevent Fraud and Identity Theft." We encourage you to remain vigilant against incidents of fraud by reviewing your account statements regularly and keeping a close eye on your credit card activity. If you see any suspicious activity, please report it to the bank that issued your credit card.

For More Information. If you have additional questions or need more information, please call our dedicated assistance line at 855-939-0541, Monday through Friday (excluding U.S. holidays), 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to AAU at P.O. Box 22409, Lake Buena Vista, FL 32830.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Dr. Roger J. Goudy
President and CEO
Amateur Athletic Union

STEPS YOU CAN TAKE TO PREVENT FRAUD AND IDENTITY THEFT

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	www.equifax.com/personal/credit-report-services

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 your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting 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 violators. 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 Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.