



July 25, 2024

SID BOSE
DIRECT NUMBER: 312-236-2243
SID.BOSE@icemiller.com

CONFIDENTIAL

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

To Whom It May Concern:

We represent Kent State University ("Kent State"), located at 310 Harbourt Hall, 615 Loop Rd., Kent, Ohio 44242, and write to notify your office of an incident that may affect the security of certain personal information relating to thirty-nine (39) Maryland residents.

Description of the Breach

Keffer Development Services, LLC ("Keffer") is a vendor that created and maintains the Athletic Trainer System (ATS). Kent State is a customer of Keffer and uses ATS for treatment management of Kent State's athletes. Keffer indicated that an account with administrative access for ATS was used by an unauthorized party and may have accessed Kent State information stored in ATS.

We understand from Keffer that the incident took place between January 2020 and January 2021. Around December 14, 2023, Keffer provided Kent State University with sufficient information to ascertain which of Kent State University's students' information may have been involved in this incident. Keffer informed us that ATS was targeted by a bad actor who gained access by using a brute-force hacking method. At no time did this incident affect Kent State University's own systems, software, or networks, and none of Kent State University's other data was involved.

Remediation Measures Taken

Kent State immediately convened an incident response team that included cybersecurity professionals to help us fully understand what happened, the population involved, and the data at stake. To best protect against future incidents, Kent State is now requiring additional security controls and protocols from Keffer, and Kent State employees who use this program have reset their passwords, following more stringent complexity requirements. Keffer has informed us that they will also be implementing additional account security controls in the near future. Additionally,



Keffer informed us that law enforcement has been working to identify the bad actor and hold them accountable.

Keffer also informed us that it was working with the Federal Bureau of Investigation in connection with this incident.

Form of Notice to Affected Individuals

Kent State provided electronic notice to the affected individuals on January 23, 2024. Kent State will be providing written notice of this incident to thirty-nine (39) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as Exhibit A.

If you require further information about this matter, please contact us by telephone at (317) 236-2243 or via email at Sid.Bose@icemiller.com.

Sincerely,

ICE MILLER, LLP

A handwritten signature in blue ink, appearing to read "Bose".

Sid Bose

Attachment: Exhibit A

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 24, 2024



K8341-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 DOMESTIC

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



[Letter Subject Line - CA Only]

Dear Sample:

Kent State University takes the privacy and security of your information seriously. We are writing to inform you about an incident that recently came to our attention and to provide you with information regarding the incident and the steps we have taken to address this matter.

Keffer Development Services, LLC ("Keffer") is a vendor that created and maintains Athletic Trainer Services (ATS), a service used by Kent State University Athletics to track training and injury status among student-athletes. Keffer discovered an incident that may affect the security of your personal information.

What Happened?

Kent State University is a customer of Keffer and uses ATS for the treatment management of Kent State University's athletes. Keffer indicated that an account with administrative access for ATS was used by an unauthorized party and may have accessed Kent State University information stored in ATS. Around December 14, 2023, Keffer provided Kent State University with sufficient information to ascertain which of Kent State University's students' information may have been involved in this incident. Keffer informed us that ATS was targeted by a bad actor who gained access by using a brute-force hacking method.

What Information Was Involved?

The information at risk includes, but may not be limited to, the following personal details:

- Name
- Date of birth
- Athletic treatment history
- COVID-19 status, including vaccinations
- [SSN Mail Merge]

What Are We Doing?

At no time did this incident affect Kent State University's own systems, software, or networks, and none of Kent State University's other data was involved. We take the privacy and security of your information seriously and trust that our service providers, vendors, and business partners, also take steps to protect your information.

Kent State immediately convened an incident response team that included cybersecurity professionals to help us fully understand what happened, the population involved, and the data at stake. To best protect against future incidents, Kent State is now requiring additional security controls and protocols from Keffer, and Kent State employees who use this program have reset their passwords, following more stringent complexity requirements. Keffer has informed us that they will also be implementing additional account security controls in the near future. Additionally, Keffer informed us that law enforcement has been working to identify the bad actor and hold them accountable.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for ## months.

ENGAGE#

0000001



K8341-L01

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. An Experian Identity Restoration agent will help you determine if identity restoration support is needed and if so, work with you to investigate and try to resolve each incident of fraud that occurred from the date of the incident. This may include, as appropriate, helping you contact credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition.

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity theft detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** October 31, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration because of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-0255 by October 31, 2024. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-918-0255 toll-free Monday through Friday from 9 a.m. to 9 p.m. Eastern (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,

Department of Intercollegiate Athletics
Kent State University

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Recommended Steps to Help Protect Your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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. N.W., Washington, D.C. 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, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



