KUTAKROCK

**Kutak Rock LLP**
The Omaha Building, 1650 Farnam Street, Omaha, NE 68102-2103
office 402.346.6000

**Todd C. Kinney**
402.346.6000
todd.kinney@kutakrock.com

August 16, 2024

**VIA EMAIL** consumer@ag.iowa.gov

RE: Security Breach Incident of ATS, a Third Party Vendor of Simpson College

To Whom it May Concern:

Pursuant to the Personal Information Security Breach Provision, **Iowa Code § 715C.1-2**, we are sending this letter to apprise the Office of the Attorney General of the State of Iowa of a security breach incident on behalf of our client, Simpson College.

On November 17, 2023, Simpson College received a letter from Athletic Trainer System ("ATS"). ATS is a third-party vendor that provides certain services to Simpson College, including, allowing certain Simpson College students to upload certain personal information, including, but not limited to, protected health information. In ATS's November 17 letter, ATS disclosed that a threat actor may have accessed and/or acquired personal information of approximately 107 Simpson College student athletes between January 2020 and January 2021.

On November 30, 2023, ATS followed up with a second letter updating the number of Simpson College student athletes who may have been affected. ATS was not able to confirm which Simpson College athlete profiles were accessed by the threat actor. We do not know for sure if the threat actor accessed any specific information of any potentially affected Simson College students.

The information involved in the attack may have included any information that a Simpson College student provided to ATS in using the service ATS provided.

ATS informed Simpson College that ATS is working to implement multi-factor authentication for user accounts to reduce the likelihood of another incident. Further, Simpson College has reminded students of the importance of strong passwords and changing passwords on a regular basis. Finally, Simpson College has also advised students that although this incident appears to have occurred more than three years ago, any students with an active student account with ATS should promptly change their username, password, and any security question(s).

The total number of Iowa individuals being notified is 2,637. Please find a sample copy of the notice letter being sent to individuals, attached.

Sincerely,

Todd C. Kinney

TCK

Simpson College
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

August 12, 2024

**Notice of Data Breach**

Dear <<First Name>> <<Last Name>>,

We are writing to you to make you aware of a recent privacy incident with a third party vendor that may have affected certain former and/or current Simpson College student athletes. We take the privacy of our students very seriously and understand that your personal information is important to you. Included in this notice are some steps you may take to help protect yourself.

**What Happened**

On November 17, 2023 Simpson College received a letter from Athletic Trainer System ("ATS"). ATS is a third party vendor that provides certain services to the College, including allowing Simpson College students to upload certain personal information, including, but not limited to, protected health information.

In its November 17 letter, ATS disclosed that a threat actor may have accessed and/or acquired personal information of approximately 107 Simpson College athletes between January 2020 and January 2021. ATS followed up with another letter dated November 30, 2023 updating the number of Simpson College student athletes who may have been affected. ATS was not able to confirm which Simpson College athlete profiles were accessed by the threat actor. Please note that we do not know for sure if the threat actor accessed your specific information. However, out of an abundance of caution, we wanted to notify you of the incident.

**What Information Was Involved**

The information involved in the attack may have included any information you provided to ATS.

**What We Are Doing**

ATS informed Simpson College that ATS is working to implement multi-factor authentication for user accounts to reduce the likelihood of another incident.

Additionally, ATS informed Simpson College that the FBI was prosecuting the threat actor and had recovered some if not all of the threat actor's devices with users' information.

We remind all Simpson College student athletes of the importance of strong passwords and changing passwords on a regular basis. Although ATS has indicated that this incident appears to have occurred more than three years ago, if you

still have an active student profile and access to the ATS software platform, Simpson College advises you to promptly change your username, password, and any security question(s).

**What You Can Do**

We encourage you to enroll in the free identity theft protection services being offered by the College through IDX, A ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identification theft recovery services.

To enroll in the program, please contact IDX at 1-888-298-3506 or visit https://app.idx.us/account-creation/protect and use the Enrollment Code provided above. Please note the deadline to enroll is November 12, 2024. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information or enrollment and are available Monday through Friday from 9am – 9pm Eastern Time.

There are additional actions you can consider to reduce the risk of identity theft or fraud on your account(s). Please refer to the enclosed **Recommended Steps** document for more information, attached to this Notice.

Again, at this time, we have no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering and reach out to the Company with any questions or concerns.

**For More Information**

You will find detailed instructions for enrollment on the enclosed **Recommended Steps** document. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

If you have any questions about the underlying incident, please feel to send an inquiry with your contact information via email to cybersecurity@simpson.edu.

Sincerely,

DAN SLOAN, MPA, CISSP
Chief Information Technology Officer

**Recommended Steps to help Protect your Information**

**1**. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at 1-888-298-3506 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. 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.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

**5. 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 | Experian Fraud Reporting | TransUnion Fraud Reporting |
|---|---|---|
| 1-866-349-5191 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348-5069 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | 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.**

**6. 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.

**7. 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.

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

**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.