EXHIBIT A

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

CONVERSE

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

March x, 2025

Dear <<first name>> <<last name>>:

Converse is reaching out to inform you of a data incident that involves some of your information that the university maintains. This correspondence provides you with information about what happened, steps we have taken in response, and steps you may take should you feel it is appropriate.

What Happened? On November 11, 2024, Converse identified unusual activity on a portion of the computer network. In response, we isolated the activity and began an investigation to determine what occurred. Through this investigation, we identified that certain files that contained information about students, alumni and employees were copied without permission. After the files were identified, we immediately engaged specialists to assist us in launching and conducting a comprehensive review of those files to identify whose information was involved, and then worked to locate contact information so that we could notify those individuals. We proceeded as expeditiously as possible, and this detailed review was complete on February 28, 2025.

What Information Was Involved? The review identified that your name and the following pieces of information were in the involved files: <<exposed data elements>>. Please note, however, that your information being contained in the files does not mean that you are the victim of identity theft of fraud, and we have no indication of an individual experiencing verified identity theft as a result of this matter. Nevertheless, if you have any concerns, we are providing you with complimentary identity monitoring and free resources as detailed below.

What We Are Doing. Following our review, we are notifying individuals to ensure they are aware of this matter. Additionally, we are providing individuals with free resources and guidance, including identity monitoring services. While no safeguards can fully prevent all cybersecurity matters, we implemented additional technical measures and processes to reduce the risk of an issue like this reoccurring. We will continue to evaluate and update our policies and practices as appropriate.

What You Can Do. You may consider remaining vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the "Steps Individuals Can Take To Protect Personal Information" section of this letter. Further, you may enroll in the complimentary identity monitoring. The enrollment instructions are in the "Enroll in Monitoring Services" section of this letter. Please note that, due to privacy restrictions, we are unable to automatically enroll you in the complimentary identity monitoring services.

For More Information. If you have questions about this matter, we have an assistance line with agents ready to answer your questions. Please contact our toll-free assistance line at 1-833-998-6161, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays. You may also write to us at Converse University, Attn: Campus Technology Department, 580 E. Main Street, Spartanburg, SC 29302.

Sincerely,

Converse University

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to this matter, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **www.mytrueidentity.com** and follow the instructions provided. When prompted, please provide the following unique code to receive services: **<<Unique Code>>**.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Ave NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General.