Attachment A

On May 24, 2024, Varsity Brands identified unusual activity on its systems. Upon detection, Varsity Brands promptly took steps to stop the activity and took certain systems offline. An investigation was launched with assistance from external cybersecurity experts. Varsity Brands also notified law enforcement.

Varsity Brands has since determined that on May 24, 2024 an unauthorized third party obtained a small subset of company files. Once Varsity Brands identified the affected files, it began a process to determine what types of personal information were affected and to whom that information relates. The affected data includes name, social security number, date of birth, government issued IDs, medical information, health insurance information, financial account information, employee ID, and checking account number.

On August 26, 2024, Varsity Brands determined that the personal information of approximately 934 Washington residents was among the downloaded files. Individual notifications sent via U.S postal mail will begin on October 14, 2024. Varsity Brands is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft restoration services. A sample individual notice is attached. Varsity Brands has established a dedicated call center to answer questions from these individuals related to this incident.

Prior to the incident, Varsity Brands had a number of security measures in place. Upon discovering the incident, Varsity Brands promptly rotated credentials, implemented additional safeguards, reinforced its security practices, and is actively reviewing its systems to further strengthen security monitoring and controls.

Varsity Brands, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

VARSITY BRANDS

October 14, 2024

Re: Notice of a Data Breach

We are writing to inform you that some of your personal information was recently impacted when we experienced a security incident. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring.

What happened?

On May 24, 2024, Varsity Brands identified unusual activity on our systems. Upon detection, we promptly took steps to stop the activity and took certain systems offline. An investigation was launched with assistance from external cybersecurity experts. We also notified law enforcement.

What personal information was involved?

After shutting down the unusual activity, we determined that an unauthorized third party obtained a small subset of company files. Once we identified the affected files, we began a process to determine whether any personal information was impacted and to whom that information relates. We recently determined that your

was among the files obtained on May 24, 2024.

What we are doing:

Prior to the incident, Varsity Brands had a number of security measures in place. Upon discovering the incident, we promptly rotated credentials, implemented additional safeguards, reinforced our security practices, and we are actively reviewing our systems to further strengthen security monitoring and controls.

We are offering you a complimentary 24-month membership to TransUnion's credit monitoring and identity theft protection services. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: January 31, 2025** (Your code will not work after this date).
- Visit the TransUnion website to enroll.
  - For Adults: www.mytrueidentity.com
  - For parent-child monitoring: https://bfs.cyberscout.com/activate
- Provide your activation code (see Attachment A)

You must enroll by January 31, 2025 to receive these services.

Please see Attachment A for additional details regarding these services.

What you can do:

It is always wise to remain vigilant against potential threats of identity theft or fraud by regularly monitoring your account statements and credit history for any signs of unauthorized activity. You can also enroll in the complimentary TransUnion service being offered to you.

Additional information about how to protect your identity and personal information is contained in Attachment B in this mailing.

For more information:

A dedicated call center has been set up to answer your questions about this incident. You may call it toll free at 1-844-428-0839, Monday through Friday 8 a.m. to 8 p.m. ET (excluding major U.S. holidays).

Sincerely,

The Varsity Brands Security Team

Encs. Attachment A
Attachment B

Attachment A - TransUnion Credit Monitoring Services

To activate your membership and start monitoring your personal information please follow the steps below:

For adults:
In response to the incident, 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 twenty-four (24) 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 the 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:**

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.

For parent-child monitoring:
In response to the incident, we are providing the parents of impacted minor dependents with access to Cyber Monitoring services for you and your minor child for twenty-four (24) months at no charge. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Cyber Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. **When prompted please provide the following unique code to receive services:** . *Once you have completed the enrollment for yourself*, click on your name in the top right of your dashboard and then "Add Family Member" to enroll your child. To complete the child's enrollment, click on the child's name and provide the requested information for monitoring.

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 an email account and will require enrollment by parent or guardian first. 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.

Attachment B - More Information about Identity Protection

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	**Experian**	**TransUnion**
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

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, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319; +1 (515) 281-5164; www.iowaattorneygeneral.gov.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (877) 566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit
https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; +1 (800)-771-7755; or www.ag.ny.gov.

For Arizona, California, Iowa, Montana, New York, North Carolina, Washington and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).