CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

ERNEST KOSCHINEG
ekoschineg@c-wlaw.com

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

Visit us online at
www.C-WLAW.com

January 7, 2022

Via Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Incident Notification

To Whom It May Concern:

We serve as counsel for Charles River Apparel ("CRA") located at 1205 Providence Highway, Sharon, MA 02067 and provide this notification to you of a recent data security incident. By providing this notice, CRA does not waive any rights or defenses under New Hampshire law, including the data breach notification statute.

On or around October 18, 2021, CRA became aware of suspicious activity related to its network and immediately began working with I.T. and third-party computer specialists to secure the network, enhance CRA's already robust security, and conduct an investigation. This included the deployment of an advanced endpoint monitoring tool. As a result of a thorough investigation, CRA discovered that limited CRA data may have been subject to unauthorized access. Upon discovery, CRA performed a thorough review of potentially impacted data to determine whether it contained any sensitive information and discovered that certain current and former employee information would be present. CRA subsequently worked to obtain up-to-date address information for current and former employees in order to provide notification. This review was completed December 15, 2021 and CRA discovered that four (4) residents of New Hampshire were potentially impacted. The information at risk includes the individuals' name and Social Security number.

On January 7, 2022, CRA is providing written notice of this incident to the New Hampshire residents pursuant to New Hampshire law. The notice letter includes an offer of complimentary credit monitoring and identity protection services offered through Kroll for 24 months. A copy of the notice letter is attached hereto.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: _____
Ernest Koschineg, Esq.

CHARLES RIVER
APPAREL

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Charles River Apparel ("CRA") is writing to inform you of a cyber incident experienced by our company that may have involved your information described below. While we have no evidence of misuse of information as a result of this incident, we are providing you with information about the incident, our response, and steps you can take to protect your information.

What Happened:

On or around October 18, 2021, we became aware of suspicious activity related to our network. We immediately began working with our I.T. team and third-party computer specialists to secure our network and conduct an investigation to determine how this incident occurred. As a result of a thorough investigation, we have discovered that limited CRA data may have been subject to unauthorized access. Upon discovery, we performed a thorough review of potentially impacted data to determine whether it contained any sensitive information and discovered that certain current and former employee information was present.

What Information Was Involved:

The information contained in the potentially affected files and data included your name in combination with your Social Security number.

What We Are Doing:

Upon discovery, we immediately secured our systems and engaged third-party computer specialists to investigate this matter. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, an online credit monitoring service for 24 months provided by Kroll. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can activate the complementary credit monitoring service we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information".

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at (855) 618-3192, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

The security of information is of the utmost importance to us, and we will continue to take steps to protect information in our care.

Sincerely,

Barry Lipsett
CEO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holiday. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

You can sign up for the online or offline credit monitoring service anytime between now and <<b2b_text_6(activation deadline)>> . Due to privacy laws, we cannot register you directly. Activating this service will not affect your credit score.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/ account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit 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, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

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

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. 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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.