BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

October 22, 2018

**VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)**
**VIA OVERNIGHT MAIL**

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

*Re: Incident Notification*

Dear Attorney General Ferguson:

We are writing on behalf of our client, Challenger Sports, Inc. ("Challenger"), the operator of ChallengerTeamWear.com, to notify you of a security incident involving Washington residents.

Challenger received reports from a small number of customers of fraudulent activity on payment cards previously used on www.ChallengerTeamwear.com (the "Website"). Challenger immediately stopped accepting payment cards on the Website, began an internal investigation, and hired a leading cyber security firm to assist. On September 12, 2018, the investigation determined that an unauthorized person gained access to Challenger's system between August 26 and August 29, 2018, and may have accessed information from purchases made on the Website from May 9, 2017 through August 29, 2018. The investigation did not determine until October 12, 2018 that information regarding Washington residents was involved. The information includes individuals' names, addresses, email addresses, order information, payment card numbers, card expiration dates, and card verification codes (CVV).

Today, Challenger will begin notifying 516 Washington residents via U.S. mail in accordance with Wash. Rev. Code § 19.255.010 in substantially the same form as the enclosed letter.[1] Challenger is advising potentially impacted individuals to remain vigilant and review their

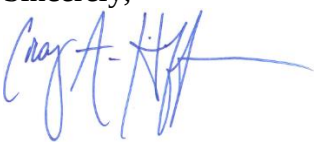
[1] This report is not, and does not constitute, a waiver of Challenger's objection that Washington lacks personal jurisdiction regarding the company related to this matter.

financial account statements for suspicious activity. Challenger is also providing a telephone number for potentially affected individuals to call with any questions they may have.

To help prevent this type of incident from happening again, Challenger forced a system-wide password change and is taking steps to strengthen the security of the Website, including by implementing additional monitoring and detection tools and security assessment scans. Challenger has informed law enforcement and will support their investigation.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Craig A. Hoffman
Partner

Enclosure

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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

Challenger Teamwear values your business and understands the importance of protecting your personal information. We are writing to inform you that we recently identified and addressed a security incident that may have involved your payment card information. This notice describes the incident, outlines the measures we have taken in response, and advises you on steps you can take to further protect your information.

When we received reports from a small number of customers of fraudulent activity on payment cards previously used on www.ChallengerTeamwear.com (the "Website"), we immediately stopped accepting payment cards on the Website, began an internal investigation, and hired a leading cyber security firm to assist us. On September 12, 2018 the investigation determined that an unauthorized person gained access to our system between August 26 and August 29, 2018 and may have accessed information from purchases made on the Website from May 9, 2017 through August 29, 2018. Because you made a purchase on the Website between May 9, 2017 and August 29, 2018, it is possible that your information was involved. This information includes your name, address, email address, order information, payment card number ending in <<ClientDef1(####)>>, the card expiration date, and the card verification code (CVV).

We remind you to remain vigilant to the possibility of fraud by reviewing your account statements for any unauthorized activity. Immediately report any unauthorized charges to your financial institution because the payment card network rules generally restrict cardholder responsibility for fraudulent charges that are timely reported. Please review the following pages for more information on additional measures you can take. To help prevent this type of incident from happening again we forced a system-wide password change and are taking steps to strengthen the security of the Website, including by implementing additional monitoring and detection tools and security assessment scans. We have informed law enforcement and will support their investigation.

We regret any inconvenience or concern this may have caused. If you have questions, please call 1-???-???-???? Monday through Friday between the hours of 8:00 a.m. and 5:30 p.m. Central Time.

Sincerely,

Paul Lawrence
CEO

## MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on your financial accounts, you should immediately contact your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

*TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

**Contact information for the Federal Trade Commission is as follows:**

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

**If you are a resident of Connecticut, Maryland, or North Carolina** you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland) or 410-576-6300 (for calls originating outside Maryland)

*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll free at 1-877-566-7226

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

*Experian Security Freeze*, PO Box 9554, Allen, TX 75013, www.experian.com

*TransUnion Security Freeze*, PO Box 2000, Chester, PA 19016, www.transunion.com

*Equifax Security Freeze*, PO Box 105788, Atlanta, GA 30348, www.equifax.com

In order 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, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit.

The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.