EASTON-BELL SPORTS

EASTON BELL Riddell GIRO BLACKBURN

Processing Center · P.O. Box 3825 · Suwanee, GA 30024

John Q. Sample, Jr.
123 Anytstreet Ave.
Apt. 123
Anytown, TX 78701

January 17, 2014

Dear John Q. Sample, Jr.,

With much regret, I am writing to make you aware that Easton-Bell Sports, Inc. ("Easton-Bell"), which includes Easton, Bell, Riddell, Giro, Blackburn and Easton Cycling, recently discovered that servers at one of our vendors were subject to a malicious software ("malware") computer intrusion. We believe the incident may have begun on December 1, 2013. The servers that were accessed contained Easton-Bell information and may impact customers who made online purchases between December 1, 2013 and December 31, 2013. [redacted] On January 9, 2014, Easton-Bell determined that this malware intrusion may have resulted in an unauthorized individual having accessed your information. Upon discovery, we immediately shut down the affected servers and took steps to prevent further access to your information, including cleaning and rebuilding the affected servers. We have also hired a highly experienced computer forensic specialist to conduct an exhaustive investigation of this matter. We are also working with our vendor on additional measures that can be taken to prevent such incidents in the future.

We realize that when you shop with us in the online environment, you put your confidence in us. We value you as our client, and we deeply regret that this incident occurred.

Although our investigation has not found that your information has been misused, we treat this matter with the utmost seriousness. For this reason, we want to make sure you have the information you need so that you can take steps to help protect yourself from identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at **no cost to you**. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use this service – there is no action required on your part. If a problem arises, simply call (866) 979-2595 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling (866) 979-2595 using the following redemption code: 9999999999.

Please note: Additional steps may be required by you in order to activate your phone alerts.

Again, this protection is being offered at no cost to you.

You can also place a fraud alert with the major credit reporting agencies on your credit files, their contact information is as follows:

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	800-525-6285	www.equifax.com
Experian	Experian Fraud Reporting P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

A fraud alert lasts 90 days, and requires potential creditors to use "reasonable policies and procedures" to verify your identity before issuing credit in your name (as soon as one agency is notified, the others are notified to place fraud alerts as well). When you contact these agencies, you can also request that they provide a copy of your credit report. Review your reports carefully to ensure that the information contained in them is accurate. If you see anything on your credit reports or credit card account statements that appear incorrect, contact the credit reporting agency or your credit card provider, and report suspected incidents of identity theft to local law enforcement, the Attorney General, or the FTC. Even if you do not find any signs of fraud on your reports or account statements, the FTC and other security experts suggest that you check your credit reports and account statements periodically. You can keep the fraud alert in place at the credit reporting agencies by calling again after 90 days.

You can also ask these same credit reporting agencies to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. 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. If you want to have a security freeze placed on your account, you must make a request in writing by certified mail to the reporting agencies. The reporting agencies will ask you for certain information about yourself. This will vary depending on where you live and the credit reporting agency, but normally includes your name, social security number, date of birth, and current and prior addresses (and proof thereof), and a copy of government-issued identification. The cost to place, temporarily lift, or permanently lift a credit freeze varies by state, but generally, the credit reporting agencies will charge $5.00 or $10.00, unless you have are the victim of identity theft who has submitted a copy of a valid investigative or incident report, or complaint with a law enforcement agency, in which case under many state laws it is free. You have the right to a police report under certain state laws.

If you detect any unauthorized charges on your credit or debit card(s), we strongly suggest that you contact your card issuer by calling the toll-free number located on the back of your card or on your monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. You should tell your card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your card web account password immediately when you discover unauthorized charges.

Finally, the FTC, your Attorney General, and the major credit reporting agencies listed above can provide additional information on how to avoid identity theft, how to place a fraud alert, and how to place a security freeze on your credit report. You can contact the FTC on its toll-free Identity Theft helpline: 1-877-438-4338. The FTC's website is located at http://www.ftc.gov/idtheft and its address is Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. In Maryland, you can reach the State Attorney General's office by phone at (888) 743-0023. Its website is http://www.oag.state.md.us/. In North Carolina, you can reach the State Attorney General's office by phone at (919) 716-6400. Its website is http://www.ncdoj.gov. Their mailing addresses are:

Douglas F. Gansler
Attorney General of the State of Maryland
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Roy A. Cooper
Attorney General of the State of North Carolina
Consumer Protection Division, Attorney General's Office
Mail Service Center 9001
Raleigh, NC 27699-9001

We are genuinely sorry that this incident occurred and apologize for any inconvenience this matter may cause you. I can assure you that we are doing everything we can to protect you – our customers – and ensure nothing like this happens again. If you have questions about this notice or this incident or require further assistance, you can reach us at (866) 892-6059, between the hours of 8:00 a.m. and 5:00 p.m. (CST). You can also get more information at http://www.eastonbellsports.com. Please reference this letter when calling.

Thank you,

Terry G. Lee
Executive Chairman & Chief Executive Officer
Easton-Bell Sports, Inc.

Easton-Bell Sports
7855 Haskell Avenue, Suite 200
Van Nuys, CA 91406

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
You are automatically protected for twelve (12) months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077