

Summit Sports—Email Notice to Affected Individuals

Subject: Important Security and Protection Notification—Please Read

I am contacting you regarding a data security incident that has occurred at Summit Sports. This incident involved a website development database storing encrypted credit card information. We believe that the encrypted credit cards may have been decoded by a hacker who also may have had access to the encryption key. As a result, it is possible that the credit card you used for your purchase at Summit Sports may have been compromised and used for fraudulent purposes. Please be assured that we have taken every step necessary to address the incident.

Details of the Data Security Incident

In late October 2011, we were contacted by an American Express fraud agent who asked us about an isolated incident involving six AmEx cards. His questions prompted us to retain a team of certified forensic IT experts to conduct an immediate investigation. Their goal was to identify, locate and secure any data vulnerabilities at Summit Sports that might exist. During this investigation, thirty customers called us to report fraudulent activity on the credit cards they had recently used for their online purchases. Every effort was made to determine the scope of the security incident and to restore the reasonable integrity of our IT system as expeditiously as possible. On December 15, 2011, these experts identified and confirmed the source of the suspected vulnerability, at which time we immediately took the source of the incident—our development server—offline. During this same period of time we implemented a new way of accepting credit cards for online sales that does not even store encrypted credit card information—it's a process that sends your credit card information to your bank for authorization, but transmits only coded "bits" or tokens back to Summit Sports to authorize your purchase. This means that our servers no longer process or store any encrypted credit card information from our customers.

What Information May Have Been Compromised and When

We cannot be sure when the hacker gained access to our development server, thus we have decided to take the overly cautious approach to notify all customers that have made purchases with us from May 2010 through December 15, 2011. We chose May 2010 based on our forensic experts' analysis of a coding change in the encryption software that was made at that time. The information that may have been compromised includes your name, email address, the credit card number of the card used for your purchase, and the billing address for that card.

Recommended Next Steps

Our recommendation to you is three-fold. First, carefully review your credit card statements (for the card you used to make your purchase with us). If you notice any unusual activity or unauthorized purchases, you should call that credit card company to cancel your card. Second, contact one of the credit reporting agencies listed below to place a fraud alert on your credit report. You don't need to have experienced fraudulent activity to place a fraud alert on your credit report. A fraud alert simply means that any new requests for credit will be subject to special scrutiny. You only need to contact one of the agencies below—the agency you contact will notify the other credit reporting agencies.

EQUIFAX

Phone: 800-525-6285

<http://www.equifax.com>

Equifax Information Services, LLC
Post Office Box 740256
Atlanta, GA 30374

EXPERIAN Phone: 888-397-3742
<http://www.experian.com/consumer/index.html>

Experian
Post Office Box 2104
Allen, TX 75013

TRANS UNION Phone: 800-680-7289
<http://www.transunion.com>

TransUnion
Post Office Box 2000
Chester, PA 19022

Third, if you haven't requested your free copy of your credit report, you can do that at the time you contact one of the above agencies to place the fraud alert on your report. Of course, for the next six months or so, you should continue to review carefully your monthly credit card statement.

More Information/Fraudulent Activity

The Federal Trade Commission (FTC) maintains a website with useful information and advice. If you have experienced actual fraudulent activity on your credit card, you should follow the steps outlined on the FTC website ([Visit the FTC's ID Theft web site](#)) and other identity theft web sites to learn more about protecting yourself now and in the future.

We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the product outlined herein. If you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at [\[insert phone number\]](#) or visit our [website FAQs](#).

Sincerely,

Steve Kopitz, President
Summit Sports