

July 21, 2023

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Portal: <https://appengine.egov.com/apps/me/maine/ag/reportingform>

Attorney General Aaron Frey
Office of the Attorney General
Attn: Security Breach Notification
Department of Professional & Financial Regulation
Bureau of Consumer Credit Protection
35 State House Station
Augusta, Maine 04333

Re: Notice of CommerceV3’s Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Creedmoor Sports, Inc., (“Creedmoor”), headquartered in 167 Creedmoor Way, Anniston, AL, 36205, with respect to a data security incident that its third party e-commerce platform, CommerceV3, Inc. (“CommerceV3”), experienced.

This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of individuals being notified, and the steps that Creedmoor has taken in response to the incident.

1. Nature of the Incident

CommerceV3 provides the e-commerce platform utilized by many online retailers to process payment card information transactions. On June 6, 2023, CommerceV3 informed Creedmoor that CommerceV3 learned that an unauthorized party obtained access to its systems between November 24, 2021 and December 14, 2022. CommerceV3 stated that upon learning of this issue, CommerceV3 conducted a thorough forensic investigation alongside third-party cybersecurity experts to assess whether any cardholder data was compromised as a result of the incident. CommerceV3 further stated that on May 3, 2023, that the forensic investigation discovered that cardholder data collected on Creedmoor’s behalf was potentially accessed or acquired by an unauthorized party as a result of the incident.

The types of information that was identified by CommerceV3 as potentially accessed and/or acquired as a result of the incident include name along with email address, billing address, payment card number, CVV code and expiration date.

2. Number of Maine residents affected.

A total of approximately 53 Maine residents have been potentially affected by this incident. Notification letters to individuals were mailed on July 21, 2023 by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Creedmoor has sent a demand to get confirmation of what steps CommerceV3 has taken. Based on CommerceV3 correspondence with Creedmoor, CommerceV3 has represented the following: CommerceV3 completed a forensic investigation and has implemented additional security measures designed to protect the privacy of our customers. CommerceV3 further stated that on December 14, 2022 the root cause of the incident was identified and remedial action was taken by CommerceV3 to ensure data is secure while using websites on their platform.

In response to being notified of this incident, Creedmoor contacted Commerce V3 immediately to ensure they, as the provider, had completed all security updates to their platform in order to protect customer data. Creedmoor is also offering complimentary credit monitoring and identity theft protection services to the potentially affected individuals. Notification letters were sent to those impacted individuals with the information to enroll in the credit monitoring services.

4. Contact information

Creedmoor Sports Inc. remains dedicated to protecting the sensitive information that is hosted by its third party vendors. If you have any questions or need additional information, please do not hesitate to contact my colleague, Karen Bridges at Karen.Bridges@WilsonElser.com or 312-706-3023.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A

Creedmoor Sports, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



July 21, 2023

Re: Notice of CommerceV3's Data Security Incident

Dear ,

Creedmoor Sports, Inc., ("Creedmoor") wants to notify you of an incident that impacted the third party e-commerce platform, CommerceV3, Inc. ("CommerceV3"), that may have involved some of your personal information.

Who is CommerceV3? CommerceV3 provides an e-commerce platform utilized by many online retailers to process payment card transactions.

What Happened? On June 6, 2023, CommerceV3 informed Creedmoor that CommerceV3 learned that an unauthorized party obtained access to its systems between November 24, 2021 and December 14, 2022. CommerceV3 stated that upon learning of this issue, CommerceV3 conducted a thorough forensic investigation alongside third-party cybersecurity experts to assess whether any cardholder data was compromised as a result of the incident. CommerceV3 further stated that on May 3, 2023, that the forensic investigation discovered that cardholder data collected on Creedmoor's behalf was potentially accessed or acquired by an unauthorized party as a result of the incident.

What Information Was Involved? CommerceV3 informed their clients that your name along with your email address, billing address, payment card number, CVV code and expiration date were **potentially** accessed and/or acquired as a result of the incident.

What CommerceV3 is Doing: Based on CommerceV3 correspondence with us, CommerceV3 has represented to us the following: CommerceV3 completed a forensic investigation and has implemented additional security measures designed to protect the privacy of our customers. CommerceV3 further stated that on December 14, 2022 the root cause of the incident was identified and remedial action was taken by CommerceV3 to ensure your data is secure while using websites on their platform.

What We Are Doing: Data privacy and security is among Creedmoor's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information of our customers. In response to being notified of this incident, we contacted Commerce V3 immediately to ensure they, as the provider, had completed all security updates to their platform in order to protect customer data.

We are also 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 **twelve (12)** 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 event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do: We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/creedmoorsports>** and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] 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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

For individuals seeking more information or questions about this incident, please call Creedmoor's dedicated toll-free helpline at **1-833-263-5863** between the hours of 8:00 am to 8:00 pm ET Monday through Friday, excluding holidays.

Once again, Creedmoor sincerely apologizes for any inconvenience this incident may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Greg Kantorovich

Greg Kantorovich
CEO
Creedmoor Sports, Inc.

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580,

www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov