20204

April 19, 2021

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]

RE: Consumer Notice of Data Breach to Massachusetts Residents

Dear Valued Blade HQ Customer,

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident on the Blade HQ websites that may involve your personal information. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected customers about the incident, and about tools you can use to protect yourself against possible fraud.

From January 7, 2021 through March 22, 2021 and on April 11, 2021, there was a potential unauthorized acquisition of your personal information at Blade HQ, LLC and its websites (bladehq.com, grindworx.com, arcform.com, or flytanium.com).

You may wonder why you are hearing about the incident now. When we first became aware of potentially unusual activity on our website in late March, we immediately hired cybersecurity experts and forensic investigators to assist in our investigation. Applicable legal requirements and best practices require that we conduct a complete investigation and cooperate and follow the required protocols of applicable governmental authorities—in certain jurisdictions we are also required by law to ensure that certain additional steps be followed before notifying customers. Now that those steps and requirements have been completed and our investigation concluded, we are reaching out to you.

What we are doing.

Blade HQ values your privacy and deeply regrets that this incident occurred. We have retained the services of a qualified cybersecurity forensic investigation firm to contain the breach, conduct a thorough review of the intrusion, and to ensure the security of the website now and in the future. We have implemented security measures to prevent a recurrence of such a security issue and to protect the privacy of our valued customers. We are also working closely with governmental authorities, to ensure that the incident is properly addressed.

What you can do.

Under Massachusetts law, you have the right to obtain any 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. Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

For More Information.

For further information and assistance, please call our response center at (855) 723-1664 Monday through Friday from the hours of 8:00 a.m. to 5:30 p.m. Central Standard Time, excluding major US holidays.

We sincerely apologize for this inconvenience and are grateful for our relationship with you. Thank you for your support of Blade HQ.

Sincerely,

Mark Christensen

CEO, Blade HQ

ADDITIONAL RESOURCES

It is recommended that you remain vigilant by reviewing account statements and monitoring your free credit reports for unauthorized activity, especially activity that may indicate fraud and identity theft.

Contact information for the three nationwide credit reporting agencies:

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

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts.

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have 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 listed above.

Security Freeze.

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com).To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348 1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

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, the addresses where you have lived over the prior five years;

5. Proof of current address,suchas a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including 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 identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide 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 between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Federal Trade Commission and Attorney General Resources.

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 home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338). To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You may also contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

Information About the Security Incident

Business name(s): Blade HQ, LLC, a Utah limited liability company (which also operates under the registered business names "ARCFORM", "Flytanium", and "Grindworx") (the "**Company**")

Type of business: online retailer of outdoor equipment

Contact: Ammon Padeken, COO, ammon@bladehq.com, 801-592-8463

Corporate headquarters
564 W 700 S #102
Pleasant Grove, Utah 84062

Nature of the incident: One or more unknown and unauthorized parties gained access to the Company's hosted server infrastructure, possibly by using a compromised admin account. The unauthorized parties appear to have uploaded malicious JavaScript code to the website in order to perform credit card transaction "skimming" operations. Potentially unusual activity on the Company's website began to be investigated on Thursday, March 18th, 2021. The Company hired a forensic cybersecurity investigation firm to investigate the unusual activity. The cybersecurity firm's investigators completed their report on April 13th, 2021, and they continue to monitor and investigate. Following investigation, it has been determined that the aforementioned JavaScript code is reasonably likely to have existed on the site from approximately January 7th, 2021 until March 22, 2021, and again for a brief period on April 11, 2021.

Types of affected information: The malicious JavaScript code potentially may have skimmed newly-entered customer transaction information during the period, including customer names, addresses, email addresses, billing and mailing addresses, credit card numbers, credit card expiration dates, and CVV codes. The Company does not collect social security numbers or other personally identifiable information. The unauthorized intrusion did not access any stored, retained or preserved customer transaction information, and the Company does not retain credit card numbers, credit card expiration dates, or CVV codes.

Perpetrator: unknown

Remedial action: The Company's IT professionals patched vulnerable security vectors immediately upon becoming aware of a potential intrusion and continued to search for and repair any other security vulnerabilities as they were discovered. The Company procured the services of a forensic cybersecurity investigatory and consulting firm to advise the Company of what, if any, malicious operations occurred and has followed the recommendations of this firm. The Company created a clean and secure server and switched all operations to such clean server. The Company has added new and increased security measures internally.

Steps to assist affected customers: The Company plans to notify the potentially affected customers from April 20, 2021 to April 30, 2021. In your state, potentially affected customers will be contacted through postal mail, or where legally permissible, by email.

The Company has procured the services of a qualified call center to field inquiries that may come from potentially affected customers, and the call center number is included on the customer notification. The Company will also provide potentially affected customers with contact information for the major credit bureaus and information regarding the process of implementing fraud alerts.

Date and timeframe of the issue: The Company noticed unusual activity on March 18, 2021 and began to investigate. The Company employed a forensic cybersecurity investigation firm on March 22, 2021 to conduct an investigation, and as of April 13, 2021, such cybersecurity firm has completed up their investigation and considers the Company's websites to be secure.

Knowledge of non-US involvement: No knowledge of non-US involvement was described in the cybersecurity investigation firm's report.

Free services to potentially-affected individuals: The Company is providing a call center to provide responsive guidance for potentially-affected customers who inquire.

Does the company maintain a written information security program: The Company has not previously maintained a written information security program or policy, but is implementing a written information security policy in consultation with cybersecurity consultants and legal counsel.

Has a report been made to law enforcement: None, other than notification of relevant state Attorney's General, other regulatory agencies, or law enforcement bodies, in each case where required by law.