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.

BLADEHQ

April 19, 2021

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

RE: Notice of Data Breach

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 (bladehq.com, grindworx.com, arcform.com, or flytanium.com) 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.

What happened?

An unknown, unauthorized intruder or intruders appears to have gained access to our hosted website servers and uploaded malware to our website www.bladehq.com, potentially gaining the capacity to "skim" customer transaction data as it was being entered by the customers purchasing or attempting to purchase our merchandise. Our investigation indicates that the intruders may have had this "skimming" capability from January 7, 2021 through March 22, 2021 and on April 11, 2021. The attackers may have gained access to customer transaction information if the customer entered new or updated information at the site during that time. Because you entered or changed your card information or personal information at bladehq.com during the suspected period of intrusion, we are notifying you about this security incident.

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 information was involved?

In the cases mentioned above, information that the intruder may have had access to includes your first and last name, address, email address, and any debit or credit card numbers with expiration dates and CVV codes that you may have entered on our website.

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. The intruder's access and malware have been removed from our website, and we have deployed new servers and implemented additional security measures to prevent a recurrence of such an attack and to protect the privacy of our valued customers. We are also working closely with major credit card suppliers and governmental authorities, to ensure that the incident is properly addressed.

What you can do.

Please also review the attachment to this letter 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.

***For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** 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. 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 one of the three national credit reporting agencies listed above.

Security Freeze. In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to request a security freeze or to remove a security freeze.

To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission, Attorneys General, and Governmental 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.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia residents. You may contact the Office of the District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001. District of Columbia residents may also wish to review information provided by the District of Columbia Attorney General on how to avoid identity theft at https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft, or by sending an email to oag@dc.gov, or calling (202) 727-3400.

For Kentucky Residents: You may contact the Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023. Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico Residents: 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 a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visitingwww.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 New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226. North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at: North Carolina Attorney General's Office, Consumer Protection Division , 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-566-7226 (Toll-free within North Carolina); 919-716-6000.

For Rhode Island residents: You may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400. You have the right to file or obtain a police report regarding the breach.

Reporting of identity theft, obtaining a police report, and certain law enforcement disclosures.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Wisconsin residents: This notice has not been delayed on the basis of any law enforcement investigation.