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.

# of residents potentially affected: 651

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.