Shawn E. Tuma
Direct Dial: 972.324.0317
stuma@spencerfane.com

September 6, 2022

Office of the Attorney General
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

via email:
consumer@ag.iowa.gov

Re: Notification of Data Security Incident

Dear Attorney General Tom Miller:

Be advised that the undersigned and this law firm have been retained to represent Ballistic Products, Inc. ("Ballistic") in connection with the recent data security incident described below.

Ballistic initially advised those potentially affected in April 2022 that one of its third-party vendors experienced a data security incident involving the presence of malware on their servers. The vendor in question provides the functionality for the shopping cart and payment processing aspects for Ballistic's and other customers' websites. According to the vendor in question, in early February 2022, the vendor was notified by another customer that malware had been identified on a server hosting that particular customer's website. The vendor informed Ballistic that it quickly commenced an investigation and identified and removed the malware found on the servers that hosted those certain customers' e-commerce websites. The vendor has since confirmed to Ballistic that the malware was removed and additional steps were taken to block the unauthorized activity. After a thorough investigation by data security experts, on July 26, 2022 it was determined that cardholders who used a credit card on Ballistic's website between September 18, 2020 and February 3, 2022 may have had some personal information impacted by the presence of the malware on the servers of the vendor. The affected information that may have been captured by the malware included information entered into the checkout page, including first and last name, payment card number, expiration date, security code, billing address, gift certificate number, and transaction details such as product type, price, and quantity purchased.

Ballistic is offering affected individuals identity theft protection services through IDX the data breach and recovery services expert. The IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

Ballistic mailed notification letters to the 532 affected Iowa residents on September 1, 2022. A sample copy of the notice each Iowa resident will receive is enclosed.

Respectfully,

Spencer Fane, LLP

By: _____
Shawn E. Tuma, Partner

Enclosure: Notice of Data Breach

P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-764-0239
Or Visit:
https://response.idx.us/ballistic-products
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<Address3>>
<<City>>, <<State>> <<Zipcode>>
<<Country>>

September 1, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

As we previously advised in April 2022, one of Ballistic Products, Inc.'s ("Ballistic") third-party vendors (the "Vendor") experienced a data security incident involving the presence of malware on their servers. Ballistic is again notifying you of the data security issue and is now providing additional information. The Vendor provides the shopping cart and payment processing functionality for various companies' e-commerce sites, including Ballistic's. According to the Vendor, in early February 2022, the Vendor was notified by another customer that malware had been identified on a server hosting that particular customer's website. The Vendor informed Ballistic that it quickly commenced an investigation and identified and removed the malware found on the servers that hosted those certain customers' e-commerce websites. The Vendor has since confirmed to Ballistic that the malware was removed and additional steps were taken to block the unauthorized activity. After a thorough investigation by data security experts, on July 26, 2022 it was determined that cardholders who used a credit card between September 18, 2020 and February 3, 2022 may have had some personal information impacted by the presence of the malware on the servers of the Vendor. While we do not have evidence that your information has been used for fraudulent purposes, we take the protection of your information very seriously and are notifying you out of an abundance of caution.

What Information Was Involved

The malware was designed to capture information entered into the checkout page, including first and last name, payment card number, expiration date, security code, billing address, gift certificate number (if applicable), and transaction details such as product type, price, and quantity purchased.

What We Are Doing

This incident has been reported to law enforcement. Additionally, as indicated above, after becoming aware of the issue the Vendor immediately took steps to identify and remove the malware and block any further unauthorized activity. The Vendor also promptly launched an extensive investigation with the assistance of data security experts to determine the timeframes of exposure for each of the Vendor's affected customers and to identify any impacted cardholders. In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-764-0239 or going to https://response.idx.us/ballistic-products and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is December 1, 2022.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-764-0239 or go to https://response.idx.us/ballistic-products for assistance or for any additional questions you may have.

Sincerely,

Grant Fackler
Ballistic Products

(Enclosure)

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://response.idx.us/ballistic-products and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-764-0239 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 visiting 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.

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/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.