LEWIS BRISBOIS BISGAARD & SMITH LLP

Richard W. Goldberg
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Richard.Goldberg@lewisbrisbois.com
Direct: 215.977.4060

May 21, 2021

File No. 44629.83

VIA E-MAIL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
E-Mail: breach.security@maine.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Defender Industries, Inc. ("Defender") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute, 10 Me. Rev. Stat. Ann. §§ 1346-1350B.

1. Nature of the Incident

On April 15, 2021, Defender became aware of malware on its e-commerce platform. Defender took immediate steps to remove the malware and notified its merchant processor as well as Visa, Mastercard, and American Express. Defender also launched an investigation and engaged a digital forensics firm to determine what happened and what information may have been accessed. On April 23, 2021, the investigation determined that this incident might have involved personal information belonging to certain Defender customers. Defender then worked diligently to identify address information associated with such customers in order to provide notification of this incident.

2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately 477 Maine residents. The information involved in the incident may include name and payment card information.

The affected individuals will receive a letter notifying them of the incident and providing steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on May 21, 2021.

3. Measures Taken to Address the Incident

Upon learning of this incident, Defender took immediate steps to remove the malware from its e-commerce platform. Additionally, Defender has notified the payment card brands and credit reporting agencies. Finally, Defender has notified the potentially impacted individuals and provided them with information about steps they can take to protect their personal information.

4. Contact Information

Defender remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 215.977.4060 or Richard.Goldberg@lewisbrisbois.com.

Sincerely,

/s/ Richard W. Goldberg

Richard W. Goldberg of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

RWG:vhn
Enclosure: Sample Consumer Notification Letter

Defender®
C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>
<<COMPANY>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

May 21, 2021

Re: Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

Defender Industries recently learned that its online payment platform had been affected by malware and that your payment card information may have been affected. Only online orders were at risk, while outlet store counter sales and contact center telephone orders were not affected. Defender strives to maintain your trust by demonstrating our continued commitment to your security and satisfaction. We are providing this information and offering information to help our customers protect their payment card data.

What Happened? On April 15, 2021, Defender learned that it was the victim of a malware incident on its e-commerce platform. Defender took immediate steps to remove the malware and notified the credit card companies so that steps could be taken to prevent unauthorized activity on any affected cards. Defender also worked with an industry-leading cybersecurity firm to assist in an investigation of what happened. On April 30, 2021, the investigation revealed that this incident might have involved your information. Defender then worked to identify address information associated with possibly affected customers in order to provide notification of this incident. In addition, we notified law enforcement about this criminal activity and will continue to provide whatever cooperation is necessary to hold the actors accountable.

The problem with the online payment system has been resolved and security measures for online ordering should prevent a similar incident from happening in the future.

What Information Was Involved? Based on our investigation, it appears that payment cards used by customers for online purchases between November 22, 2020 and April 15, 2021 may be involved. The affected payment card information may have included names, addresses, credit card information, and email addresses.

What We Are Doing? As soon as we discovered this incident, we took the measures referenced above and took steps to help prevent a similar incident from occurring in the future. We also notified payment card networks so that they can coordinate with card issuing banks to monitor for unauthorized activity on cards used during the identified timeframe.

What You Can Do? We encourage you to carefully review and monitor your payment card account statements. We are also offering information about steps you can take to help protect your personal information. Please read the recommendations included with this letter which you can follow.

For More Information. If you have any questions regarding the incident, please call 833-664-2017. We deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Defender Industries, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.