Blundstone
TASMANIA AUSTRALIA·1870
317 George St, Ste 515
New Brunswick, NJ 08901-2008

September 14, 2024

M0312-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of Data Breach

Dear Sample A. Sample,

Blundstone U.S.A., Inc. ("**Blundstone**," "**we**," "**our**," "**us**") recently experienced a security incident that may have impacted your personal information. On August 16, 2024, we sent you an email notice about this same incident to help you start taking any appropriate precautions. This letter provides additional information about what happened and the steps you can take in response.

**What Happened?**
Blundstone uses the Adobe Commerce (formerly Magento) platform to power Blundstone's e-commerce website. On August 15, 2024, we learned that an unauthorized third party had exploited a vulnerability in the Adobe Commerce platform that allowed this third party to install malicious code that duplicated a Blundstone webpage at the point of sale. This duplicated checkout webpage then enabled the third party to collect contact and payment information entered during online transactions on our website. When we learned of this incident, we took immediate steps to secure our systems. Additionally, we launched an investigation of the incident with the support of a leading outside cybersecurity firm and experienced legal counsel. Our investigation determined that this unauthorized third party was able to access personal information between July 7, 2024, and August 14, 2024.

**What Information Was Involved?**
We determined that the information affected may have included some or all of the following information about you: first and last name; billing address(es); shipping address(es); phone number; and/or payment card information, including number, expiration date, and Card Verification Value ("CVV") code.

**What We Are Doing.**
Blundstone has removed the malicious code from our systems. In addition, we applied security patches to resolve the vulnerability on the external Adobe Commerce platform. We have instituted additional technical practices to reduce the risk of similar incidents occurring in the future.

**What You Can Do.**
It is always advisable to remain vigilant against attempts at fraud or identity theft, which includes carefully reviewing online and financial accounts and credit reports for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

**Other Important Information.**
Additional information about how to protect your information is contained in Attachment A.

**For More Information.**
Blundstone deeply regrets that this incident occurred and is committed to continue working to prevent these types of events from occurring in the future. If you have any questions regarding this incident, please contact our data privacy team at dataprivacy@blundstone.com or 1-800-437-2526.

Sincerely,

Ailsa Sypkes
Blundstone, Group Manager Legal & Compliance

## Attachment A – Information for U.S. Residents

Below are additional helpful tips you may want to consider to protect your personal information.

**Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. 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 law enforcement, the Federal Trade Commission, and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the Federal Trade Commission at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

**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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

| Equifax: | Experian: | TransUnion: |
|---|---|---|
| equifax.com | experian.com | transunion.com |
| equifax.com/personal/credit-report-services | experian.com/help | transunion.com/credit-help |
| P.O. Box 740241 | P.O. Box 2002 | P.O. Box 1000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19016 |
| 800-685-1111 | 888-397-3742 | 888-909-8872 |

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

**Fraud Alert**

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

**Security Freeze**

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Consumer reporting agencies have three business days after receiving your request to place a security freeze, or one business day for requests made electronically or by toll-free telephone. They must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) and/or password that can be used to authorize the removal or lifting of the security freeze.

Consumer reporting agencies must lift a security freeze within three business days after receiving your request by mail, or one hour after receiving your request electronically or by toll-free telephone. To remove or temporarily lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail or electronically, and include: proper identification (name, address, and Social Security number); the PIN or password provided to you when you placed the security freeze; and the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

**Federal Fair Credit Reporting Act Rights**
The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the Federal Trade Commission has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 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 violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

**Additional Information**
If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

**For Colorado and Illinois residents**: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

**For Iowa residents**: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

**For Maryland residents**: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

**For New York residents**: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

**For New Mexico Residents**: You have rights pursuant to the FCRA, 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 FCRA, the consumer reporting bureaus 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 violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA 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 Avenue NW, Washington, DC 20580.

**For North Carolina residents**: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. The North Carolina Attorney General may be able to provide you with information about preventing identity theft.

**For Oregon residents**: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click "How to get a security freeze."

**For Rhode Island residents**: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are 27 Rhode Island residents impacted by this event.

**For Washington, D.C. residents:** You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, http://oag.dc.gov, 1-202-727-3400. The Office of the Attorney General for the District of Columbia may be able to provide you with information about the steps you can take to avoid identity theft.

**For Arizona, California, Iowa, New York, North Carolina, Oregon, Washington, and Washington, D.C.:** 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 bureaus directly to obtain such additional report(s).