Blundstone

TASMANIA AUSTRALIA·1870

317 George St, Ste 515
New Brunswick, NJ 08901-2008

September 14, 2024

M0312-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02 MT
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, which includes carefully reviewing your online and financial accounts 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, and reset your password as an extra precaution.

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.

Sincerely,

Ailsa Sypkes
Group Manager, Legal & Compliance
Blundstone