Adam Brune – ALPS Brands
4575 HWY 185 New Haven, MO 63068
573.459.2577 - FAX 573.459.2044
E-mail adam@alpsbrands.com
www.alpsbrands.com

March 23, 2021

INTENDED FOR ADDRESSEE(S) ONLY

VIA US MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

On behalf of Active Lifestyle Products & Services, Inc., d/b/a as ALPS Brands ("ALPS"), I am writing to notify your office of an incident that may affect the security of certain personal information of forty-two (42) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ALPS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 25, 2021, ALPS discovered a potential security concern with its website(s) (including, www.alpsbrands.com, www.alpsmountaineering.com, www.alpsoutdoorz.com, www.browningcamping.com, www.hikerdirect.com, and www.alpscedarridge.com, collectively referred to herein as the "Websites"). ALPS moved swiftly to engage a service provider to investigate the issue. The next day, February 26, 2021, the service provider that ALPS engaged to investigate the Websites confirmed that ALPS systems had been unlawfully accessed by an unknown third party. The affected systems were immediately disabled while ALPS and its service provider conducted an investigation of the issue to determine if any customer information had been compromised. Our technology systems have since been secured and restored to working order.

An unknown attacker unlawfully breached the e-commerce portion of the Websites and installed a malicious program that attempts to capture data related to certain credit card transactions. This malicious program only works on live transactions as they take place. ALPS does not keep or store credit card information. Our investigation indicated that this software was installed as far back as April 20, 2020. The transaction data captured by the attack included the following personal information: the customer's first and last names, email address, mailing address and credit card information, including the credit card number, the expiration date, and the CVV code for such card. These transaction data included credit card

transactions with forty-two (42) New Hampshire residents. ALPS does not collect through the e-commerce portion of the Websites any social security numbers or protected health information, and so this information was not collected in the attack. ALPS is implementing security measures to prevent a recurrence of such an attack and to protect the privacy of our valued customers.

Notice to New Hampshire Residents

On or about March 23, 2021, ALPS will begin providing written notice of this incident to affected individuals, which includes forty-two (42) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as Exhibit A.

Other Steps Taken and To Be Taken

As soon as ALPS and its service provider recognized there may be a problem, they took steps to investigate the problem, stop the attack and mitigate any damage caused by the attack. We are working with the applicable governmental officials to ensure the incident is properly reported and addressed. This notice was not delayed as a result of a law enforcement investigation.

Additionally, as part of the notice provided to the affected individuals, ALPS is providing guidance on how the impacted individuals may protect against identity theft and fraud, including advising the individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. ALPS is also providing such individuals with (i) information on how to place a fraud alert and security freeze on their credit file, (ii) information on protecting against tax fraud, (iii) the contact details for the national consumer reporting agencies, (iv) information on how to obtain a free credit report, (v) a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and (vi) encouragement to contact the Federal Trade Commission, their state's Attorney General, and/or law enforcement agencies to report any attempted or actual identity theft and fraud.
ALPS will continue to take the steps necessary to protect its customers, their personal information and ALP's information technology environments.

Contact Information

Should you have any questions regarding this notification or other aspects of the incident, please contact ALPS using the below contact information.

Mail:	**Phone:**	**Online:**
ALPS Brands 4575 Highway 185 New Haven, MO 63068	800.344.2577 (M–F, 8am–4:30pm CST)	https://www.alpsbrands.com/contact

Very truly yours,
Adam Brune, Vice President

EXHIBIT A

ALPS Brands
4575 HWY 185 New Haven, MO 63068
573.459.2577 - FAX 573.459.2044
www.alpsbrands.com

TO: Affected Customers of Active Lifestyle Products & Services, Inc.

FROM: Active Lifestyle Products & Services, Inc.

DATE: _____, 2021

NOTICE OF DATA BREACH

We, at Active Lifestyle Products & Services, Inc., d/b/a as ALPS Brands ("ALPS"), value and respect the privacy of your information, which is why we are writing to inform you of a data security incident that has occurred.

WHAT HAPPENED?

On February 25, 2021, ALPS discovered a potential security concern with its website(s) (including, www.alpsbrands.com, www.alpsmountaineering.com, www.alpsoutdoorz.com, www.browningcamping.com, www.hikerdirect.com, and www.alpscedarridge.com, collectively referred to herein as the "Websites"). ALPS moved swiftly to engage a service provider to investigate the issue. The next day, February 26, 2021, the service provider that ALPS engaged to investigate the Websites confirmed that ALPS systems had been unlawfully accessed by an unknown third party. The affected systems were immediately disabled while ALPS and its service provider conducted an investigation of the issue to determine if any customer information had been compromised. Our technology systems have since been secured and restored to working order.

WHAT INFORMATION WAS INVOLVED?

An unknown attacker unlawfully breached the e-commerce portion of the Websites and installed a malicious program that attempts to capture data related to certain credit card transactions. This malicious program only works on live transactions as they take place. ALPS does not keep or store your credit card information. Our investigation indicated that this software was installed as far back as April 20, 2020.

The transaction data captured by the attack included the following personal information: the customer's first and last names, email address, mailing address and credit card information, including the credit card number, the expiration date, and the CVV code for such card. Please be rest assured that ALPS does not collect through the e-commerce portion of the Websites any social security numbers or protected health information, and so this information was not collected in the attack.

WHAT WE ARE DOING

ALPS values your privacy and deeply regrets that this incident occurred. We are conducting a thorough review of the incident, and will notify you if there are any significant developments. We engaged a service provider to review and secure the system, and we are implementing additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of our valued customers. We are working with the applicable governmental officials to ensure the incident is properly reported and addressed. This notice was not delayed as a result of a law enforcement investigation.

WHAT YOU CAN DO

Please also review the Steps You Can Take to Further Protect Your Information attachment for further information on steps you can take to protect your information.

FOR MORE INFORMATION

For further information and assistance, please contact ALPS using the below contact information.

Mail:	**Phone:**	**Online:**
ALPS Brands 4575 Highway 185 New Haven, MO 63068	800.344.2577 (M–F, 8am–4:30pm CST)	https://www.alpsbrands.com/contact

Steps You Can Take to Further Protect Your 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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you 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 can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

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 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. 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.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information.

Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/501a-identity-theft-a-recovery-plan_2018.pdf.

D.C. residents can obtain information from the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft at 400 6th Street, NW, Washington, DC 20001, (202) 727-3400, or https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

New York residents may receive information regarding security breach response and identity theft prevention and protection information from (i) the New York Attorney General at https://ag.ny.gov/consumer-frauds/identity-theft or (518) 776-2000, (ii) the Division of State Police Department of State's Division of Consumer Protection at https://www.dos.ny.gov/consumerprotection/ or (800) 697-1220, or (iii) the Office of Information Technology Services' Enterprise Information Security Office at https://its.ny.gov/ciso or 518-242-5045.

North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General online at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/, at North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, or by calling 877-566-7226 (Toll-free within North Carolina) or 919-716-6000.

OTHER IMPORTANT INFORMATION

- **Security Freeze**

Under 15 U.S.C. Section 1681c-1, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

- **Your Rights Under the Federal Fair Credit Reporting Act**

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 violator. You 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. We encourage you to review your rights pursuant to the Fair Credit Reporting by visiting www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W. Washington, DC 20552.

- **Police Report**

You also have the right to file a police report in the location in which the offense occurred or the city or county in which you reside.