



Dear [customer name],

We care about the security of your personal information, and we are providing the notice below to tell you that we have discovered evidence of unauthorized access to some of your personal information.

<p>VF Outdoor, LLC doing business as The North Face® 1551 Wewatta Street Denver, CO 80202</p> <p>November 5, 2020</p>	
NOTICE OF DATA BREACH	
What Happened?	<p>We care about the security of your personal information, and we are writing to tell you that we have discovered evidence of unauthorized access to some of your personal information. On October 9, 2020, we were alerted to unusual activity involving our website, thenorthface.com, that prompted us to investigate immediately. Following a careful investigation, we concluded that a credential stuffing attack had been launched against our website on October 8 and 9, 2020. A “credential stuffing attack” is a specific type of cybersecurity attack in which the attacker uses account authentication credentials (e.g., email addresses/usernames and passwords) stolen from another source, such as a breach of another company or website, to gain unauthorized access to user accounts. Credential stuffing attacks can occur when individuals use the same authentication credentials on multiple websites, which is why we encourage you to use a unique password on thenorthface.com.</p> <p>Based on our investigation, we believe that the attacker previously gained access to your email address and password from another source (not from The North Face) and subsequently used those same credentials to access your account on thenorthface.com.</p> <p>We do not believe that the attacker obtained information from us that would require us to notify you of a data security breach under applicable law, but we are notifying you of the incident voluntarily, out of an abundance of caution.</p>
What Information Was Involved?	<p>Based on our investigation, we believe that the attacker obtained your email address and password from another source (as described above) and may have accessed the information stored on your account at thenorthface.com, including products you have purchased on our website, products you have saved to your “favorites,” your billing address, your shipping address(es), your VIPeak customer loyalty point total, your email preferences, your first and last name, your birthday (if you saved it to your account), and your telephone number (if you saved it to your account).</p> <p>If you saved your payment card (credit, debit or stored value card) to your account on thenorthface.com, the attacker was not able to view your payment card number, expiration date, nor your CVV (the short code on the back of your card), because we do not keep a copy of that information on thenorthface.com. We only retain a “token” that we have linked to your payment card, and only our third-party payment card processor retains payment card details. The token cannot be used to initiate a purchase</p>

	anywhere other than on thenorthface.com. Accordingly, your credit card information is not at risk as a result of this incident.
What We Are Doing.	Please know that protecting your personal information is something that we take very seriously. Once we became aware of the incident, we quickly took steps to address the incident, including by implementing measures that limit account logins from sources that we believe are suspicious or in patterns that are suspicious. As a further precaution, we disabled all passwords from accounts that were accessed during the timeframe of the attack. We also erased all payment card tokens from all accounts on thenorthface.com. As such, you will need to create a new (unique) password and enter your payment card information again the next time you shop on thenorthface.com. We want to assure you that the safety of your information on our website is our utmost concern.
What You Can Do.	<p>Other than the use of your email address and password to access your account, we are not aware of any fraudulent activity conducted using your information on thenorthface.com. Nevertheless, as described above, we have reason to believe that some of your personal information was compromised in the past from another source, so we encourage you to take steps to reduce the potential risk of misuse of your online accounts. Please change your password at thenorthface.com and at all other sites where you use the same password. <u><i>We strongly encourage you not to use the same password for your account at thenorthface.com that you use on other websites, because if one of those other websites is breached, your email address and password could be used to access your account at thenorthface.com.</i></u> In addition, we recommend avoiding using easy-to-guess passwords. You should also be on alert for schemes, known as “phishing” attacks, where malicious actors may pretend to represent The North Face or other organizations, and you should not provide your personal information in response to any electronic communications regarding a cybersecurity incident. We have included below further information on steps you may consider taking to protect your credit.</p> <p>You should monitor your financial accounts for any suspicious activity. For more information about steps you can take to reduce the likelihood of identity theft or fraud, call 1-877-ID-THEFT (877-438-4338), visit the FTC’s website at http://www.ftc.gov/bcp/edu/microsites/idtheft/, or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. However, if you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state’s attorney general, or the FTC.</p> <p>The Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly. To monitor your credit accounts, you can 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 print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.</p>
<p>Other Important Information.</p> <p style="text-align: center;">Information on Credit Report Fraud Alerts</p> <p>You may also place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You can call any one of the three major credit</p>	

bureaus at the contact information below or place fraud alerts online at the websites below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

	Experian	Equifax	TransUnion
Phone	1-888-397-3742	1-800-525-6285	1-800-680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division PO Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.experian.com/fraud/center.html	https://www.equifax.com/personal/credit-report-services/	https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

Information on Security Freezes

In addition to a fraud alert, you may place a security freeze on your credit file. A security freeze will block a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. The fees for placing a security freeze vary by state, and a consumer reporting agency may charge a fee of up to \$10.00 to place a freeze or lift or remove a freeze in some states.

To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online.

	Experian	Equifax	TransUnion
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.experian.com/freeze/center.html	https://www.equifax.com/personal/credit-report-services/	https://www.transunion.com/credit-freeze

For More Information.	Call us at 1-833-346-5227.
------------------------------	----------------------------