Dear [customer name],

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

VF Outdoor, LLC doing business as [The North Face® or Timberland®] 1551 Wewatta Street Denver, CO 80202 [date]	
NOTICE OF DATA BREACH	
What Happened?	We are writing to tell you that we have discovered evidence of unauthorized access to some of your personal information. On March 13, 2025, we were alerted to unusual activity involving our website, [thenorthface.com or timberland.com], ("**Website**"), that prompted us to investigate immediately. Following a careful investigation, we concluded that an attacker had launched a small-scale credential stuffing attack against our Website on March 13, 2025. A "credential stuffing attack" is a specific type of cybersecurity where 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. We encourage all of our customers to use a unique password on our Website. Based on our investigation, we believe that the attacker previously gained access to your email address and password from another source (not from us) and then used those same credentials to access your account on our Website. 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. However, we are notifying you of the incident voluntarily, out of an abundance of caution.
What Information Was Involved?	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 our Website. This information may include products you have purchased on our Website, your shipping address(es), your preferences, your email address, your first and last name, your date of birth (if you saved it to your account), and your telephone number (if you saved it to your account). If you saved your payment card (credit, debit, or stored value card) to your account on our Website, the attacker could not view your payment card number, expiration date, or your CVV (the short code on the back of your card). This is because we do not keep a copy of that information on our Website. We only retain a "token" linked to your payment card, and only our third-party payment card processor keeps payment card details. The token cannot be used to initiate a purchase anywhere other than on our Website. Accordingly, your credit card information is not at risk due to 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 it. These steps included disabling passwords. As such, if you have not done so already, you will need to create a new (unique) password on our Website.
What You Can Do.	Please change your password on our Website and other sites where you use the same password. ***We strongly encourage you not to use the same password for your account at our Website that you use on other websites. If a breach occurs on one of those other websites, an attacker could use your email address and password to access your account at our Website.*** 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 us or other organizations. 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. The Federal Trade Commission (FTC) recommends that you remain vigilant by checking your credit reports periodically. Regularly checking your credit reports can help you spot problems and address them quickly. You can also order free copies of your annual reports through www.annualcreditreport.com. You should also 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). You may also visit the FTC's websites at www.consumer.ftc.gov/topics/identity-theft or www.identitytheft.gov, or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. If you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state attorney general, or the FTC. Notification was not delayed as a result of a law enforcement investigation.
For More Information.	Call us at [insert number].