January 19, 2022

RE: Important notice about your account on Timberland.com and your personal information

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.

What happened?

On November 5, 2021, we were alerted to unusual activity involving our website, timberland.com, 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 October 24, 2021. A "credential stuffing attack" is a specific type of cybersecurity attack 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 timberland.com. We do not believe that the incident involved information 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.

Based on our investigation, we believe that the attacker previously gained access to your email address and password from another source (not from Timberland) and then used those same credentials to access your account on timberland.com.

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 timberland.com. 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).

Payment card (credit, debit, or stored value card) information was **not** compromised on timberland.com. *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 timberland.com. 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 timberland.com. ***Accordingly, your credit card information is <u>not</u> at risk as a result of this incident.***

What have we done to protect you?

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 and erasing payment card tokens from accounts that were accessed during the attack timeframe. As such, you will need to create a new (unique) password and enter your payment card information again the next time you shop on timberland.com.

Our investigation indicates that payment card information was saved to your account at timberland.com. A transaction was processed through timberland.com on your account during the timeframe of the attack. We promptly cancelled the transaction and refunded the total amount charged to your payment card. You should see the refund in your payment card statement. As described above, the attacker could not view your payment card details on timberland.com and your payment card information was not compromised in this incident. However, as described above, we have reason to believe that some of your personal information was compromised in the past from another source. We encourage you to take steps to reduce the potential risk of misuse of your online accounts.

Please change your password at timberland.com and other sites where you use the same password**.** ***<u>We strongly encourage you not to use the same password for your account at timberland.com 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 timberland.com.</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 Timberland 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.

How can you get more information?

For further information about this incident, you may call us at 1-888-802-9947. As described in more detail below, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

Sincerely,

VF Outdoor, LLC
doing business as Timberland®
1551 Wewatta Street
Denver, CO 80202

HOW TO PROTECT YOURSELF FROM CYBERSECURITY ATTACKS AND IDENTITY THEFT

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.

Information on Free Credit Reports

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. 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

Information on Credit Report Fraud Alerts

You may also place a fraud alert on your credit file free of charge. 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 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 or 1-888-766-0008	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** major consumer reporting agency 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

State-Specific Information

If you are a resident of the following states, the following information applies to you.

For residents of New York, North Carolina or Rhode Island: For information on how to avoid identity theft or to contact your state's attorney general, please use the below information.

New York Attorney General	North Carolina Attorney General	Rhode Island Attorney General
1-800-771-7755 https://ag.ny.gov/ Office of the Attorney General The Capitol Albany, NY 12224-0341	1-877-566-7226 http://www.ncdoj.gov Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001	(401) 274-4400 http://www.riag.ri.gov/ Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903

For residents of Rhode Island: Under Rhode Island law, you have the right to obtain a police report filed concerning this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Based on our investigation to date, we believe this incident affected forty-eight (48) individuals.