VANS

September __, 2022

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

We care about the security of your personal information. We are providing the notice below to tell you that we have discovered evidence indicating possible unauthorized access to your account on vans.com, what has been done to protect you, and what you can do now as an additional safety precaution.

What happened?

On August 20, 2022, we detected unusual activity on our website, vans.com. Following a careful investigation, we concluded that an attacker launched a credential stuffing attack against our website, vans.com, on August 19 and 20, 2022. 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), often obtained from another source, such as a breach of another company, system, or website, to gain unauthorized access to user accounts.

What information was involved?

Based on our investigation, we believe that the attacker obtained your email address and password and may have accessed the information stored on your account at vans.com. This information may include products you have purchased on our website, your billing address(es), 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), your telephone number (if you saved it to your account), the unique ID number we assigned to you, the date your account was created, your gender (if you saved it to your account), and your Vans Family reward records (if you were a Vans Family member).

Payment card (credit, debit, or stored value card) information was not compromised on vans.com. *The attacker **could not** view a full payment card number, expiration date, or a CVV (the short code on the back of your card).* We do not keep a copy of payment card details on vans.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 vans.com.** *Accordingly, even if you had saved your credit card information to your account, that information is not at risk as a result of this incident.*

What have we done to protect you?

Protecting your personal information is something that we take very seriously. Once we became aware of the attack, we quickly took steps to halt the attack. 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 vans.com. We are continuing to monitor our systems for suspicious activity.

What can you do now?

Please change your password at vans.com and other sites where you use the same password**.** ***We strongly encourage you not to use the same password for your account at vans.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 vans.com.*** 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 Vans 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, please call us at 1-833-825-1970 or email us at se_care@vans.com. 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 Vans®
1551 Wewatta Street
Denver, CO 80202

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

To protect yourself from 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

Location-Specific Information

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

For residents of Washington, D.C., Maryland, 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.

District of Columbia Attorney General	1-202-727-3400 https://oag.dc.gov/ Office of the Attorney General for the District of Columbia 441 4th Street NW

	Suite 1100 South Washington, D.C. 20001
New York Attorney General	1-800-771-7755 https://ag.ny.gov/ Office of the Attorney General The Capitol Albany, NY 12224-0341 1-800-697-1220 www.dos.ny.gov New York Department of State Division of Consumer Protection One Commerce Plaza, 99 Washington Ave. Albany, NY 12231
North Carolina Attorney General	1-877-566-7226 http://www.ncdoj.gov Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001
Rhode Island Attorney General	(401) 274-4400 http://www.riag.ri.gov/ Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903
Maryland Attorney General	1-888-743-0023 https://www.marylandattorneygeneral.gov/ Maryland Attorney General's Office 200 St. Paul Place Baltimore, MD 21202

For residents of Rhode Island and Massachusetts: 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 32,082 individuals in the United States.