WARBY PARKER

December 21, 2018

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

To Whom It May Concern:

On behalf of JAND Inc. d/b/a Warby Parker ("Warby Parker"), this letter provides notice of a computer data security incident. We send this letter as a courtesy, since the number of residents notified pursuant to Iowa Code Ann. § 715C.2, 239, approximately 239 customers in your state, is below the stated threshold. We have notified approximately 869 additional customers in your state pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5).

Warby Parker is an eyeglasses retailer that operates through its website at warbyparker.com, and at 87 retail stores in various parts of the United States. On November 26, 2018, Warby Parker became aware of unusual attempted log-in activity on its website. We began to investigate with the assistance of outside experts. Based on our investigation to date, we believe that unauthorized persons first obtained a number of usernames and passwords from other, unrelated websites that were presumably breached. We believe the unauthorized persons then attempted to log in to Warby Parker customer accounts, likely acting on the supposition that some consumers were using these same usernames and passwords across multiple websites.

To be clear, we have seen no indication that the usernames and passwords used in these log-in attempts were obtained from Warby Parker's own systems. Likewise, we have seen no proof that any personal information stored on our customers' accounts was actually obtained. The exact nature of the personal information stored in user accounts can vary from consumer to consumer. The range of data elements potentially available through the unauthorized access here included name, email, prescription information if that information was stored on the customer's account, mailing address if provided by the user, and the last four digits of any payment card information stored on the user's account. Only the last four digits are visible even to legitimate customers; accordingly, we see no scenario in which this incident would have resulted in unauthorized access to either the full payment card number or CVV number. A stored payment card number can be used to order eyewear at warbyparker.com, but cannot be used elsewhere.

On or about November 30, Warby Parker began to require that potentially affected users reset their passwords upon log-in. Warby Parker also has reported the matter to the Federal Bureau of Investigation. We now believe the unauthorized log-in attempts began on or about September 25, 2018 and continued until the investigation began two months later.

Warker Parker will notify customers in your state whose usernames and passwords may have been used to access their accounts. We began sending notice via U.S. Mail and email on or about December 20. A sample customer notification letter is attached.

To be clear, we are notifying all potentially affected customers in an excess of caution, whether or not there is proof of actual unauthorized access to their account.

Warby Parker takes the protection of its customers' data seriously, and is committed to answering any questions that your office may have. Please do not hesitate to contact me at the address above or at 646-668-3801.

Respectfully yours,

/s/

Jill Savage
Senior Counsel

Enclosures

WARBY PARKER

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
R835401

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 21, 2018

Dear John,

We are writing to tell you about a recent incident involving your Warby Parker online account. We've learned that unauthorized parties obtained usernames and passwords from other companies' security breaches, and tried to use those usernames and passwords to log in to some Warby Parker accounts. We want you to know what happened, as well as the steps we are taking to protect your personal information.

WHAT HAPPENED?
Our team noticed unusual efforts to log in to Warby Parker customer accounts. We began to investigate immediately, and so far we've determined that unauthorized parties may have obtained your username and password elsewhere—most likely through security breaches at other companies—and may have used this information to attempt to log in to your Warby Parker account. Login attempts were made to a limited number of Warby Parker accounts from late September to late November 2018.

We're notifying all customers whose accounts may have been accessed. We don't know for sure that yours was, but we would rather be safe than sorry.

WHAT ARE WE DOING?
Our security team took immediate steps to remediate this event, and is working to try to prevent this kind of event from occurring in the future. We engaged third-party cybersecurity experts to help, and we continue to monitor our site traffic closely. We have also reported this matter to law enforcement and are actively cooperating with them.

We have required all potentially affected customers to reset their passwords. If you've logged in recently, you were required to reset your password. If you haven't logged in recently, you'll be required to reset your password next time you do.

WHAT INFORMATION WAS INVOLVED?
The information involved depends on what you had in your Warby Parker account. Information that these unauthorized persons may have been able to access includes:

- your first and last name
- email address (at Warby Parker, that's also your username)
- any prescription information you had stored
- the last four digits of your payment card number, if you made a purchase with us in the past and stored the card number (note that your full payment card information was not viewed and could not have been obtained to use elsewhere)

If you had a payment card stored on your account, the unauthorized users may have been able to place an order on your warbyparker.com account.

WHAT YOU CAN DO

- Log in to your account at www.warbyparker.com to review your order history carefully. Please let us know right away if you see any activity you don't recognize.
- Reset your password upon your next login if you haven't already done so.
- If you've used the same username and password elsewhere, we strongly recommend that you change your password there, as well. Make it different from your Warby Parker login information.
- Create strong passwords, not just for your Warby Parker account. Use a combination of uppercase and lowercase letters, numbers, and other characters. And you shouldn't use the same password across multiple websites.

FOR MORE INFORMATION

If you would like to take additional steps to protect your personal information, attached to this letter are helpful tips on how to do so.

We take our responsibility to protect your information extremely seriously, and we are very sorry for any inconvenience that this has caused you. If you have any questions, please email us at privacyhelp@warbyparker.com or give us a call at 888.330.9553. We're here to help.

Sincerely,

The Warby Parker team

Keeping Your Information Safe

At Warby Parker, we take your security seriously and encourage you to do the same. The resources below can help.

Credit Reports and Identity Theft Resources

- **Order Your Free Credit Report.** To obtain an annual free copy of your credit reports, visit **annualcreditreport.com**, call toll-free at 1-877-322-8228, or contact the major credit reporting agencies. Their contact information is as follows:

Equifax:	**Experian:**	**TransUnion:**
equifax.com	**experian.com**	**transunion.com**
https://www.equifax.com/personal/credit-report-services	**experian.com/freeze**	**transunion.com/freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-888-909-8872

- You may place a fraud alert on your file by contacting one of these credit reporting agencies. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. Placing a fraud alert can protect you, but also may cause a delay when you seek to open a new account.

- You have the ability to place a security freeze on your file as well. A security freeze prevents credit, loans, and certain services from being approved in your name without your consent. Like a fraud alert, it also may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above. You may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past 5 years; proof of current address, such as a utility bill or telephone bill; a copy of a government-issued identification card; and, if you are the victim of identity theft, any police report, investigative report, or complaint to a law enforcement agency.

- If you suspect identity theft, you can file a report to your local police department or other law enforcement agency, the U.S. Federal Trade Commission (FTC), or your state Attorney General.

- **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents**: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

  For Massachusetts and Rhode Island residents: You have the right to file a police report regarding any privacy incident in which you were involved, and to obtain a copy of the report.

Helpful Contacts

- You can learn more by contacting the FTC or your state's Attorney General to obtain information including about how to avoid identity theft, place a fraud alert, and place a security freeze on your credit report.

  Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-5338), www.ftc.gov/idtheft

- **Maryland, North Carolina and Rhode Island** residents may also contact these agencies for information on preventing and avoiding identity theft:

    - **For Maryland residents**: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

    - **For North Carolina residents**: North Carolina Office of the Attorney General, Mail Service Center 9001, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.

    - **For Rhode Island residents**: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Federal Fair Credit Reporting Act Rights. The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and you may seek damages from FCRA violators. Identity theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

If you have any questions about the security of your Warby Parker account,
please email us at privacyhelp@warbyparker.com.