U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Eastern & Caribbean Region
Jacob Javits Federal Bldg.
26 Federal Plaza ● New York, NY 10278
Voice - (800) 368-1019 ● TDD – (800) 537-7697
Fax - (212) 264-3039 ● http://www.hhs.gov/ocr

September 5, 2024

VIA EMAIL (chris.utecht@warbyparker.com), CERTIFIED MAIL (RETURN RECEIPT REQUESTED), and PERSONAL SERVICE

Chris Utecht, General Counsel
Warby Parker, Inc.
233 Spring St., 6th Floor East
New York, NY 10013

Re: OCR Transaction Number: 19-327224

NOTICE OF PROPOSED DETERMINATION

Dear Chris Utecht:

Pursuant to the authority delegated by the Secretary of the United States Department of Health and Human Services ("HHS") to the Office for Civil Rights ("OCR"), I am writing to inform you that OCR is proposing to impose a civil money penalty ("CMP") of $1,500,000 against Warby Parker, Inc. (formerly known as JAND, Inc. d/b/a Warby Parker) ("Warby Parker").

This proposed action is being taken under the regulations promulgated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), § 262(a), Pub.L. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, Public Law 111-5, Section 13410, codified at 42 U.S.C. § 1320d-5, at 45 Code of Federal Regulations (C.F.R.) Parts 160 and 164.

I. The Statutory Basis for the Proposed CMP

The Secretary of HHS is authorized to impose a CMP (subject to the limitations set forth at 42 U.S.C. § 1320d-5(b)) against any covered entity, as described at 42 U.S.C. § 1320d-1(a), that violates a provision of Part C (Administrative Simplification) of Title XI of the Social Security Act. *See* HIPAA, § 262(a), as amended, 42 U.S.C. § 1320d-5(a). This authority includes imposing CMPs for violations of the applicable provisions of the Federal Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (ePHI) (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules), and the Breach Notification Rule (45 C.F.R. Parts 160 and 164, Subpart D). The

Secretary has delegated enforcement responsibility for the HIPAA Rules to the Director of OCR. *See* 65 Federal Register (Fed. Reg.) 82381 (Dec. 28, 2000) and 74 Fed. Reg. 38630 (July 27, 2009). OCR is authorized under the HITECH Act § 13410, 42 U.S.C. § 1320d-5(a)(3),[1] to impose CMPs for violations occurring on or after February 18, 2009,[2] of:

- A minimum of $100 for each violation where the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.

- A minimum of $1,000 for each violation due to reasonable cause and not to willful neglect, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $100,000. Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

- A minimum of $10,000 for each violation due to willful neglect and corrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $250,000.

- A minimum of $50,000 for each violation due to willful neglect and uncorrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

As required by law, OCR has adjusted the CMP ranges for each penalty tier for inflation. The adjusted CMP amounts apply to penalties assessed on or after August 8, 2024, if the violation occurred on or after November 2, 2015.[3]

---

[1] The CMPs reflect the penalty tiers described in the Notification of Enforcement Discretion (April 30, 2019). See https://www.federalregister.gov/documents/2019/04/30/2019-08530/notification-of-enforcement-discretion-regarding-hipaa-civil-money-penalties.

[2] For violations occurring on or after November 2, 2015, HHS may make annual adjustments to the CMP amounts pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvement Act of 2015 Sec. 701 of Public Law 114-74. The annual inflation amounts are found at 45 C.F.R. §102.3. For the most recent amounts, see 89 Fed Reg. 64815 (August 8, 2024).

[3] *Id.*

OCR is precluded from imposing a CMP unless the action is commenced within six years from the date of the violation.[4]

II. Findings of Fact

1. Warby Parker, Inc. (formerly known as JAND, Inc. d/b/a Warby Parker) ("Warby Parker") is a Delaware public benefit corporation, headquartered in New York City. It is a manufacturer and e-retailer of prescription and non-prescription eyewear. Warby Parker has approximately 200 physical stores and employs over 3,000 people.

2. Warby Parker is a health care provider that transmits health information in electronic form in connection with a transaction for which HHS has adopted standards.

3. Warby Parker is a covered entity as defined at 45 C.F.R. § 160.103, and, therefore, is required to comply with the HIPAA Rules.

4. On November 26, 2018, Warby Parker became aware of unusual login attempts on its website. Subsequently, Warby Parker learned that, from September 25, 2018, through November 30, 2018, its website was subjected to a credential stuffing attack that resulted in one or more unauthorized third parties gaining access to certain Warby Parker customer accounts.

5. On December 20, 2018, Warby Parker filed a breach report with OCR concerning the unauthorized access to its customer accounts from September 25, 2018, through November 30, 2018. As amended on September 18, 2020, the breach report stated that the ePHI of 197,986 individuals was affected by this breach. The affected ePHI included customer names, mailing addresses, email addresses, the last four digits of any payment card information stored on the customer's account, and for 177,890 of the individuals, eyewear prescription information.

6. On September 16, 2019, OCR notified Warby Parker, in writing, of its commencement of an investigation into this breach and Warby Parker's compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

7. In September 2019, January 2020, April 2020, and June 2022, Warby Parker experienced subsequent credential stuffing attacks, resulting in further unauthorized login activity leading to the breach of protected health information for 484 customers' accounts.

[4] *See* 42 U.S.C. § 1320a-7a(c)(1); 45 C.F.R. § 160.414.

8. The evidence collected during OCR's investigation finds that, to date, Warby Parker has failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI it held (*see* 45 C.F.R. § 164.308(a)(1)(ii)(A)).

9. OCR's investigation finds that Warby Parker did not implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level until July 29, 2022 (*see* 45 C.F.R. § 164.308(a)(1)(ii)(B)).

10. OCR's investigation finds that Warby Parker failed to implement procedures to regularly review records of information system activity review, such as audit logs, access reports, and security incident tracking reports until May 12, 2020 (*see* 45 C.F.R. § 164.308(a)(1)(ii)(D)).

11. On March 14, 2024, OCR notified Warby Parker of the results of OCR's investigation and offered Warby Parker an opportunity to resolve the matter informally.

12. On May 15, 2024, pursuant to 45 C.F.R. § 160.312(a)(3), OCR sent Warby Parker a Letter of Opportunity (LOO). The LOO informed Warby Parker that OCR's investigation found preliminary indications that Warby Parker failed to comply with certain provisions of the Security Rule, and that this matter had not been resolved by informal means despite OCR's attempts to do so. The LOO stated that pursuant to 45 C.F.R. § 160.312(a)(3), OCR is providing Warby Parker with an opportunity to submit written evidence of any mitigating factors (45 C.F.R. § 160.408) or affirmative defenses (45 C.F.R. § 160.410) for OCR's consideration in determining a civil money penalty (CMP) pursuant to 45 C.F.R. § 160.404. The letter also advised Warby Parker that it may submit written evidence to support a waiver of a CMP pursuant to 45 C.F.R. § 160.412. Each act of noncompliance under the Security Rule was described in the letter.

13. Warby Parker responded to the LOO on June 14, 2024.

14. OCR determined that the information and arguments submitted by Warby Parker do not support an affirmative defense pursuant to 45 C.F.R. § 160.410. See Section IV below.

15. OCR considered factors pursuant to 45 C.F.R. § 160.408, including Warby Parker's LOO response alleging a mitigating factor, based on evidence obtained by OCR during its investigation, in determining the amount of the CMP. See Section V below.

16. OCR determined that the information and arguments submitted by Warby Parker do not support a waiver of the CMP pursuant to 45 C.F.R. § 160.412. See Section VII below.

17. On August 13, 2024, OCR obtained the authorization of the Attorney General of the United States, pursuant to 42 U.S.C. § 1320a-7a, prior to issuing this Notice of Proposed Determination (NPD) to impose a CMP.

III. Basis for CMP

Based on the above findings of fact, OCR has determined that Warby Parker is liable for the following violations of the HIPAA Security Rule and, therefore, subject to a CMP:

1. To date, Warby Parker has not conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI it held, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

2. Warby Parker did not implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level until July 29, 2022, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

3. Warby Parker failed to implement procedures to regularly review records of information system activity review, such as audit logs, access reports, and security incident tracking reports until May 12, 2020, in violation of C.F.R. § 164.308(a)(1)(ii)(D). OCR has determined that the appropriate penalty tier for this violation is reasonable cause.

IV. No Affirmative Defenses

By its LOO, dated May 15, 2024, OCR offered Warby Parker the opportunity to provide written evidence of affirmative defenses per 45 C.F.R. § 160.410.

OCR determined that the information contained in Warby Parker's response, dated June 14, 2024, did not provide a basis for an affirmative defense under 45 C.F.R. § 160.410.

V. Factors Considered in Determining the Amount of the CMP

1. In determining the CMP amount, OCR is required to consider certain factors listed in the regulation at 45 C.F.R. § 160.408, which may be mitigating or aggravating as appropriate. As such, OCR considered the following:

a. *45 C.F.R. § 160.408(a) The nature and extent of the violation*.

Warby Parker's 2018 breach affected 197,986 individuals. While this breach affected a large number of individuals, it is not among the largest breaches annually reported to OCR.

Moreover, OCR's investigation identified three longstanding violations of the Security Rule. Two of these violations (Risk Management and Information Security Activity Review) were only addressed during this OCR investigation, while one (Risk Analysis) remains unaddressed by Warby Parker.

As such, OCR has determined to apply this factor as neither aggravating nor mitigating.

b. *45 C.F.R. § 160.408(b) The nature and extent of the harm resulting from the violation*.

There is no evidence that the violations of the HIPAA Security Rule resulted in physical, financial, or reputational harm, or hindered an individual's ability to obtain healthcare.

However, the fact that there is no evidence of harm cannot be attributed to any actions by Warby Parker such that would justify mitigating the CMP.

Therefore, OCR finds that this is neither an aggravating nor mitigating factor.

c. *45 C.F.R. § 160.408(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity*.

OCR has not identified any previous matters involving Warby Parker that would demonstrate whether the current violations are the same or similar to previous indications of noncompliance. However, the evidence from this investigation revealed longstanding noncompliance with Security Rule standards that were not previously reported to OCR.

As such, OCR has determined to apply this factor as neither aggravating nor mitigating.

d. *45 C.F.R. § 160.408(d) The financial condition of the covered entity*.

There is no evidence to suggest that Warby Parker had financial difficulties that would affect its ability to comply with the requirements of HIPAA, such

as costs associated with a HIPAA compliance program that would include workforce training, implementation of policies and procedures, safeguards, etc.

Furthermore, after reviewing financial documentation filed by Warby Parker with the SEC, OCR finds that the payment of a CMP would not jeopardize Warby Parker's ability to provide healthcare services.

As such, OCR has determined to apply this factor as neither aggravating nor mitigating.

e. *45 C.F.R. § 160.408(e) Such other matters as justice may require*.

OCR did not identify any other matters as justice may require. As such, OCR has determined to apply this factor as neither aggravating nor mitigating.

2. Recognized Security Practices (RSPs): Public Law 116-3218 requires that OCR consider RSPs that HIPAA covered entities adequately demonstrate had been in place for a period of not less than the previous 12 months when determining a civil money penalty.

On January 12, 2024, OCR provided an opportunity for Warby Parker to adequately demonstrate that it had RSPs in place. Warby Parker responded to OCR's request on February 5, 2024. Upon examination of all the data, policies and procedures, OCR determined that Warby Parker's response did not adequately demonstrate that it had substantially implemented RSPs in the previous 12 months. Therefore, OCR did not apply a reduction to the CMP.

VI. Waiver

OCR has determined that there is no basis for waiver of the proposed CMP amount as set forth at 45 C.F.R. § 160.412. Warby Parker presented no evidence that the payment of the CMP would be excessive relative to the violations found here and described in OCR's May 15, 2024, letter to Warby Parker.

VII. Amount of CMP

A. Amount of CMP Per Violation. Based on the above factors, OCR finds that Warby Parker is liable for the following CMPs for each violation described in Section III:

1. Risk Analysis (45 C.F.R. § 164.308(a)(1)(ii)(A)): OCR will begin calculations for this proposed violation 6 years prior to the NPD date. The

total CMP is $700,000. The appropriate penalty tier for this violation is Reasonable Cause.

i. Calendar Year 2018: 90 days from October 3, 2018, to December 31, 2018, at $1,424 per day (Total CMP of $128,160, capped at $100,000)

ii. Calendar Year 2019: 365 days at $1,424 per day (Total CMP of $519,760, capped at $100,000)

iii. Calendar Year 2020: 366 days at $1,424 per day (Total CMP of $521,184, capped at $100,000)

iv. Calendar Year 2021: 365 days at $1,424 per day (Total CMP of $519,760, capped at $100,000)

v. Calendar Year 2022: 365 days at $1,424 per day (Total CMP of $519,760, capped at $100,000)

vi. Calendar Year 2023: 365 days at $1,424 per day (Total CMP of $519,760, capped at $100,000)

vii. Calendar Year 2024: 275 days from January 1, 2024, to October 1, 2024, at $1,424 per day (Total CMP of $391,600, capped at $100,000)

Total CMP: $3,119,984, capped at $700,000

2. Risk Management (45 C.F.R. § 164.308(a)(1)(ii)(B)): OCR will begin calculations for this proposed violation 6 years prior to the NPD date. The total CMP is $500,000. The appropriate penalty tier for this violation from is Reasonable Cause.

i. Calendar Year 2018: 90 days from October 3, 2018, to December 31, 2018, at $1,424 per day (Total CMP of $128,160, capped at $100,000)

ii. Calendar Year 2019: 365 days at $1,424 per day (Total CMP of $519,760, capped at $100,000)

iii. Calendar Year 2020: 366 days at $1,424 per day (Total CMP of $521,184, capped at $100,000)

iv. Calendar Year 2021: 365 days at $1,424 per day (Total CMP of $519,760, capped at $100,000)

v. Calendar Year 2022: 210 days from January 1, 2022, to July 29, 2022, at $1,424 per day (Total CMP of $299,040, capped at $100,000)

Total CMP: $1,987,904, capped at $500,000

3. Information System Activity Review (45 C.F.R. § 164.308(a)(1)(ii)(D)): OCR will begin calculations for this proposed violation 6 years prior to the NPD date. The total CMP is $300,000. The appropriate penalty tier for this violation is Reasonable Cause.

i. Calendar Year 2018: 90 days from October 3, 2018, to December 31, 2018, at $1,424 per day (Total CMP of $128,160, capped at $100,000)

ii. Calendar Year 2019: 365 days at $1,424 per day (Total CMP of $519,760, capped at $100,000)

iii. Calendar Year 2020: 133 days from January 1, 2020, to May 12, 2020, at $1,424 per day (Total CMP of $189,392, capped at $100,000)

Total CMP: $837,312, capped at $300,000

Total CMP for all violations: $1,500,000

VIII. Right to a Hearing

Warby Parker has the right to a hearing before an administrative law judge to challenge these proposed CMPs. To request a hearing to challenge these proposed CMPs, Warby Parker must mail a request, via certified mail with return receipt requested, under the procedures set forth at 45 C.F.R. Part 160 within 90 days of your receipt of this letter. Such a request must: (1) clearly and directly admit, deny, or explain each of the findings of fact contained in this notice; and (2) state the circumstances or arguments that you allege constitute the grounds for any defense, and the factual and legal basis for opposing the proposed CMP. *See* 45 C.F.R. § 160.504(c). If you wish to request a hearing, you must submit your request to:

U.S. Department of Health & Human Services
Departmental Appeals Board, MS 6132
Civil Remedies Division
330 Independence Ave, SW
Cohen Building, Room G-644
Washington, D.C. 20201
Telephone: (202) 565-9462

Copy to:
Linda C. Colón, Regional Manager
Office for Civil Rights
U.S. Department of Health and Human Services
26 Federal Plaza, Room 19-501
New York, NY 10278
Telephone: (212) 264-4136
Email: Linda.Colon@hhs.gov

A failure to request a hearing within 90 days permits the imposition of the proposed CMP without a right to a hearing under 45 C.F.R. § 160.504 or a right of appeal under 45 C.F.R. § 160.548. ***If you choose not to contest this proposed CMP, you should submit a written statement accepting its imposition within 90 days of receipt of this notice.***

If Warby Parker does not request a hearing within 90 days, then OCR will notify Warby Parker of the imposition of the CMP through a separate letter, including instructions on how to make payment, and the CMP will become final upon receipt of such notice.

If you have questions regarding this matter, please contact Ms. Emily Crabbe, Senior Advisor for HIPDC Compliance and Enforcement, at (404) 562-7878 or via email at Emily.Crabbe@hhs.gov.

Sincerely,

/s/

Linda C. Colón
Regional Manager

cc: Iliana Peters, Legal Counsel
(via email only, **REDACTED**)