# Seeing is Believing: A Civil Money Penalty With Warby Parker Following Cybersecurity Incident

Bruce D. Armon

Published 02/26/2025

---

On February 20, 2025, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a $1.5 million civil money penalty (CMP) against Warby Parker, Inc. (WP). WP is a manufacturer and online retailer of prescription and non-prescription eyewear. The CMP was finalized on December 11, 2024 but was not announced until last week.

The CMP related to violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

**What You Need to Know:**

- Cybersecurity remains an important issue for HIPAA-covered entities.
- Regular monitoring of ePHI consistent with the HIPAA Security Rule requirements is imperative.
- It is too soon to determine if the Trump Administration will continue to negotiate settlements or impose CMPs with respect to HIPAA compliance issues.

In December 2018, OCR initiated an investigation following receipt of a breach report filed by WP. In November 2018, WP became aware of unusual, attempted log-in

activity on its website. Over a 2+ month period in the Fall of 2018, WP reported that unauthorized third parties gained access to WP customer accounts by using usernames and passwords obtained from other, unrelated websites that were presumably breached. OCR noted this type of cyberattack is often referred to as "credential stuffing".

The WP breach affected 197,986 individuals, and the compromised ePHI included customer names, mailing addresses, email addresses, certain payment card information, and eyewear prescription information. WP filed subsequent breach reports (each breach report affecting fewer than 500 persons) in April 2020, and June 2022, following similar attacks.

OCR's investigation found evidence of three violations of the HIPAA Security Rule: a failure to conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities; a failure to implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level; and a failure to implement procedures to regularly review records of information system activity.

In September 2024, OCR issued a Notice of Proposed Determination seeking to impose a $1.5 million civil money penalty. WP waived its right to a hearing and did not contest OCR's imposition of a civil money penalty. In December 2024, OCR imposed a civil money penalty of $1.5 million.

The OCR Notice of Proposed Determination explained the factors considered by OCR in determining the amount of the CMP. The Notice of Final Determination noted that WP waived its right to request a hearing from the Notice of Proposed Determination.

In its press release announcing the WP CMP, OCR noted there are multiple steps that health care providers, health plans, clearinghouses, and business associates can take to mitigate or prevent cyber-threats, including:

- Identify where ePHI is located in the organization, including how ePHI enters, flows through, and leaves the organization's information systems.
- Integrate risk analysis and risk management into the organization's business processes.
- Implement regular reviews of information system activity.

- Utilize mechanisms to authenticate information to ensure only authorized users are accessing ePHI.
- Encrypt ePHI in transit and at rest to guard against unauthorized access to ePHI when appropriate.
- Incorporate lessons learned from incidents into the organization's overall security management process.
- Provide workforce members with regular HIPAA training that is specific to the organization and to the workforce members' respective job duties.

It is too early in the Trump Administration to know if its HHS OCR leadership will continue to aggressively pursue HIPAA Security and Privacy Rule alleged violations by Covered Entities. It is clear, however, the cybersecurity threats are not a political issue. For business (and perhaps political) reasons, all covered entities and their business associates need to stay vigilant against emerging and ongoing cybersecurity activities by 'bad actors' to protect their PHI and ePHI.

## Author


Bruce D. Armon

Partner

**(215) 972-7985** | ✉

**View bio**


## Related Industries

Health Care

HIPAA / Health Information Privacy & Security