

## Report on Patient Privacy Volume 24, Number 6. June 27, 2024 Patient Privacy Court Case: June 2024

---

By Roshni Edalur

On May 30, the U.S. District Court for the Eastern District of Michigan was set to hold a final fairness hearing<sup>[1]</sup> to approve a \$2.9 million class-action lawsuit settlement against Wright & Filippis (W&F) related to a ransomware attack in January 2022.<sup>[2]</sup> W&F is a Michigan-based provider of prosthetics, orthopedics and accessibility solutions.

In January 2022, an unauthorized user launched a ransomware-type cybersecurity attack on W&F's network and computer systems.<sup>[3]</sup> W&F's security software detected the attack but was unable to prevent file encryption. The forensic investigation confirmed that the attackers had access to parts of its network containing the protected health information of more than 877,500 individuals, including names, dates of birth, patient numbers, Social Security numbers, driver's license numbers or state IDs, financial account numbers and/or medical health insurance information. Plaintiffs filed a class action and alleged that W&F was negligent due to the failure to implement reasonable and appropriate security measures to protect patients' sensitive data, and then unnecessarily delayed issuing breach notifications. While W&F denied the allegations, plaintiffs alleged they had suffered an injury as a result of the negligent acts, including theft of their information, identity theft, imminent injury from fraud, damages from delayed notifications, out-of-pocket expenses, lost time mitigating the effects of the data breach and increased costs related to reductions in their credit scores, including higher costs for borrowing and insurance.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)