

Report on Patient Privacy Volume 21, Number 11. November 11, 2021 In Plea, UPMC Hacker Sentenced to Seven Years for Conspiracy, Identity Theft

By Jane Anderson

A Pennsylvania man who hacked the personnel records of the University of Pittsburgh Medical Center (UPMC) and dangled personally identifiable information (PII) for sale on the dark web was sentenced Oct. 18 to seven years in prison for conspiracy to defraud the United States and aggravated identity theft.^[1] Chief U.S. District Judge Mark Hornak imposed the maximum allowed sentence on 30-year-old Justin Sean Johnson for the incident, which affected the PII of more than 65,000 UPMC employees.

According to the U.S. attorney's office, "Johnson, known on the dark web as TheDearthStar and Dearthly Star, infiltrated and hacked into the UPMC human resource server databases in 2013 and 2014 and stole sensitive PII and W-2 information belonging to tens of thousands of UPMC employees. Johnson then sold the stolen information on dark web forums for use by conspirators, who promptly filed hundreds of false 1040 tax returns in 2014 using UPMC employee PII. These false 1040 filings claimed hundreds of thousands of dollars of false tax refunds, which they converted into Amazon.com gift cards, which were then used to purchase Amazon merchandise which was shipped to Venezuela."

In addition, Johnson sold nearly 90,000 sets of PII unrelated to UPMC on the dark web between 2014 and 2017. "The scheme resulted in approximately \$1.7 million in false tax return refunds," the U.S. attorney's office said.

Because it was not technically a HIPAA breach—the data didn't come from patients—the incident wasn't reported on the so-called "Wall of Shame" maintained by the HHS Office for Civil Rights, and notification to federal officials and the media wasn't required. State laws do apply, however, and UPMC did alert employees.^[2]

But HIPAA officials know there is little difference in vulnerability and profit between information known as PII and protected health information (PHI), and it's highly likely that there was crossover between employees and UPMC patients, as the system includes 21 hospitals and operates an insurance plan with 2.3 million members.

Johnson was indicted and arrested in 2020. Before Johnson's sentencing, his attorney, Nicola Henry-Taylor, argued that "Johnson did not profit in any meaningful way as a result of his misconduct and only made a few thousand dollars from the sale of PHI."^[3] Henry-Taylor said that Johnson, who had been homeless at times and had little family support, turned to hacking computers because he was "desperate to meet his basic needs."

According to the attorney's office, "in imposing the sentence, Judge Hornak noted the severity of Mr. Johnson's crimes, likening his behavior to a 'bulldozer' through people's personal lives when he 'indiscriminately' hacked their PII."

Johnson had been planning the hack for at least several months, as the original indictment noted he opened a bitcoin account on Oct. 31, 2013. And UPMC may not have been his first (or only) target. As the indictment states, Johnson discussed with others gaining access to a human resources (HR) database "of a prominent national retailer." Further, the indictment alleges that as recently as 2017, Johnson had hacked into colleges and also had stolen data from "a large healthcare provider in Georgia and Florida."

To hack UPMC, Johnson studied Oracle's PeopleSoft, a suite of HR and business applications, according to the U.S. attorney's office. "Investigators years later uncovered Johnson's 'PeopleSoft expertise,' having studiously searched for PeopleSoft over 1,100 times on his computer," the U.S. attorney's office wrote in its sentencing memo. A forensic review of Johnson's laptop revealed PII from Pruitt Health Care in Georgia and Lexington Medical Center in South Carolina, the sentencing memo said, noting that "the common denominator was a PeopleSoft HR network."

1 Department of Justice, U.S. Attorney's Office for the Western District of Pennsylvania, "Judge Sentences Michigan Man to 7 Years in Prison for Hacking UPMC HR Databases and Stealing Employees' Personal Information," news release, October 18, 2021, <https://bit.ly/3bQu4tv>.

2 Theresa Defino, "Seven Years After PA Hospital Breach, Alleged Hacker Arrested; Class Action Suit Lives On," *Report on Patient Privacy* 20, no. 7 (July 2020), <https://bit.ly/3CWG2xy>.

3 United States of America v. Justin Sean Johnson, Case 2:20-cr-00094 (W.D. Penn. October 8, 2021).

This publication is only available to subscribers. To view all documents, please log in or purchase access.

[Purchase Login](#)