COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 7. July 09, 2020 Seven Years After PA Hospital Breach, Alleged Hacker Arrested; Class Action Suit Lives On

By Theresa Defino

How much would a cybercriminal pay for a person's name and other information to commit identity fraud? How does $3 sound? That's how much the Department of Justice (DOJ) alleges that Justin Sean Johnson, 29, charged when he dangled the information of thousands, if not tens of thousands of people for sale on the dark web.

Johnson was only in his early 20s when he allegedly masterminded the hack of the University of Pittsburg Medical Center (UPMC) seven years ago, according to his recent 43-count indictment.[1] The indictment also lays out in chilling detail how Johnson taught himself the weaknesses of UPMC's human resources (HR) system and made a series of exfiltrations of data, beginning on the first day of December in 2013. He was arrested June 18 and remained in custody as of *RPP's* deadline.

UPMC ultimately determined that data for all its workers (past and present, as many as 65,000 individuals) had likely been seen and possibly stolen, including Social Security numbers, dates of birth, salaries and other "highly sensitive, personally-identifiable information," also known as PII.

The IRS issued $1.7 million in fraudulent refunds to at least two individuals who filed 1,327 returns for the 2013 tax year using pilfered UPMC employee data, according to their 2017 plea agreements. Then, using the option in TurboTax to accept refunds in the form of codes for Amazon purchases, they later bought high-end electronics that were shipped to Venezuela by way of Miami and were resold in South America.

Because it was not technically a HIPAA data breach—the data didn't come from patients per se—the incident wasn't reported on the so-called "Wall of Shame" maintained by the HHS Office for Civil Rights (OCR), and notification to federal officials and the media wasn't required. (For a look at reported breaches so far this year, see story, p. 1).[2] State laws do apply, however, and UPMC did alert employees.

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 people who were also UPMC patients, as the system includes 21 hospitals and operates a 2.3 million-member insurance plan.