UPMC: All 62K employees hit in data breach

By Alex Nixon

TRIBLIVE

| Business

Hackers may have stolen Social Security numbers and other sensitive data from all 62,000 UPMC (University of Pittsburg Medical Center) employees, more than double the number reported by the hospital giant.

UPMC declined to say Friday what led investigators to expand the number of affected employees, up from 27,000 in April.

The largest hospital network in Western Pennsylvania, which is the state's biggest private employer, said authorities informed it that the breach of a payroll system was more extensive than previously thought.

“Recent developments in the ongoing investigation suggest that the scope may be larger than originally thought, potentially affecting every employee,” according to an email from UPMC to employees that the Tribune-Review obtained.

“The information stolen several months ago may include names, Social Security numbers, addresses, salary information, and even bank account information.”

The U.S. Attorney's Office in Pittsburgh, which is coordinating the investigation with the Internal Revenue Service, Secret Service, U.S. Postal Inspection Service and police, declined to comment on the development.

In a written statement, the office said “investigators are working diligently to advance the investigation.”

The number of victims of tax fraud resulting from the breach increased. UPMC said 817 employees were affected by fraud, up from 788 in April.

The hospital system has said that it learned of the breach this year when employees reported that someone filed fraudulent tax returns using their identities.

UPMC spokeswoman Gloria Kreps said there have been no other data breaches beyond the initial one, which was limited to a payroll system and did not affect patient data.

“This breach affected our payroll system, which is completely separate from patient financial and medical information,” she said.

UPMC is offering fraud detection services to all employees for free, the email stated, and is working to extend coverage for five years. UPMC asked workers to contact their banks about the theft.

“Please be assured that we have done all that we can to make sure our systems are secure, and we do not believe that a similar attack would be successful in the future,” the email to employees stated.

The breach led a UPMC employee to file a lawsuit in state court seeking class action status and 25 years of credit and bank monitoring, credit restoration services and identity theft insurance.

Alice Patrick, a dialysis clinician at UPMC McKeesport, alleges in the lawsuit that UPMC was negligent in protecting its payroll data. Patrick's attorney, Sunshine R. Fellows, could not be reached for comment.

When a thief files a faulty tax return to claim someone else's refund, the victim can retrieve his or her money by following an IRS process, according to the agency.

The health system has emphasized identify theft is a common crime, with 1.6 million taxpayers affected by the offense in the first six months of 2013. That's up from 271,000 for all of 2010, according to an audit by the Treasury Department's inspector general.

Though identity theft and data breaches are common, theft of payroll data by hackers is relatively rare, said Larry Ponemon, president and founder of Ponemon Institute, a Traverse City, Mich.-based organization that researches cybercrime issues. More commonly stolen are credit card and transaction records held by retailers, such as the theft of millions of credit card records from Target last year.

“Typically, it's a patient record or payment record in health care (that's stolen),” he said. “Rarely is it employee data. Employee data tends to be better protected.”

The size of the breach of employee data at UPMC is unique, Ponemon said.

“It's huge,” he said. “If you have most of your employees at risk, that's unusual. ... That should be a big concern.”