OnlineAthens
Athens Banner-Herald

Athens Orthopedic won't pay for extended credit monitoring in data breach

August 12, 2016 - The hacker who infiltrated the computer system at **Athens Orthopedic Clinic** "has attempted to extort the clinic for ransom money," the business said in a prepared statement released late Friday, August 12, 2016.

In the same prepared statement, the clinic also said it would not pay for extended credit monitoring for the thousands of victims of the hack, two of whom indicated in a Friday story in the Athens Banner-Herald story they were dissatisfied with the clinic's response to the data breach.

"Many patients are upset and frustrated with the situation ...," Kayo Elliott, CEO of Athens Orthopedic Clinic, said in the statement. "And of course, they wish we could pay for extended credit monitoring. So do we. We truly regret that we are unable to do so, as we are not able spend the many millions of dollars it would cost us to pay for credit monitoring for nearly 200,000 patients and keep Athens Orthopedic as a viable business. I recognize and am truly sorry for the position this puts our patients in."

According to previous information from the clinic, the hack occurred on June 14, 2016, and the clinic became aware of it on June 27. In letters mailed to the affected patients earlier this week the clinic said, "We believe that the information taken includes your name, address, Social Security number, date of birth, telephone number and account number, and may include your diagnosis and medical history."

Subsequently, the clinic released a statement saying "no patient banking information was/is stored on our system so your banking information is not affected."

In the Friday statement, the clinic notes "patients who were seen by physicians or providers who may or may not still be a part of our various locations" should be vigilant for possible indications that their personal information was part of the data breach.

According to the spokeswoman, the delay in getting the letters out to affected patients was the result of the clinic's efforts to identify which of their patients were affected by the data breach, and then ensuring the clinic had accurate mailing addresses for the notifications, which are required under the federal Health Insurance Portability and Accountability Act (HITECH Act.

Information on the hack was reported in the media, noted on social media and placed on the clinic's website well in advance of the letters being mailed out, the Friday statement notes.

Prior to Friday, the clinic indicated only that the hacker gained access to its medical records by using the log-in credentials of "a third-party vendor." The contractor was terminated following discovery of the breach, according to the clinic. In the Friday statement, the clinic provides some additional information, saying the vendor is a "nationally-known healthcare information management contractor."

Following discovery of the breach, Athens Orthopedic Clinic brought in a cybersecurity team to determine its source and to improve the clinic's computer system. Additionally, the clinic has been working with the FBI as an investigation of the hack is moving forward, according to the Friday statement. Also in the Friday statement, Athens Orthopedic says it "engaged IT and security experts to maintain, test and improve its system" prior to the data breach.

In the letter sent to patients affected by the data breach, Athens Orthopedic Clinic advises them to contact one of the three major credit reporting bureaus, Experian, Equifax or TransUnion, to place a fraud alert on their credit report. The prepared statement urges affected patients to "do this as soon as possible." The statement goes on to suggest that affected patients can seek other assistance through the Federal Trade Commission's IdentityTheft.gov website, where identity theft can be reported, or through www.clark.com, the website of popular consumer advocate Clark Howard. As Athens Orthopedic continues to struggle with the fallout from the data breach, two law firms on opposite sides of the country are investigating the possibility of pursuing a class-action lawsuit against the business.

Both Seattle-based Keller Rohrback and Conshohocken, Pa.-based Goldman Scarlato & Penny issued news releases soliciting contact from people who received letters from Athens Orthopedic Clinic advising them that their personal information was compromised, or who are concerned they might otherwise be a victim of the data breach, to contact their offices.

A Friday afternoon telephone call to Goldman Scarlato & Penny was not immediately returned, and a paralegal at Keller Rohrback referred detailed questions about that firm's efforts to the attorney handling the case, who was out of the office on Friday.

In its news release, Goldman Scarlato & Penny notes its "attorneys are actively litigating data breach actions" against a number of healthcare companies and other entities. The release goes on to note that people affected by data breaches "should be concerned about identity theft." Stolen information can, according to the law firm, be "used to file false tax returns, make fraudulent claims for health care coverage, open credit accounts in the name of the victim, and more."

Article posted here: http://onlineathens.com/mobile/2016-08-12/athens-orthopedic-wont-pay-extended-credit-monitoring-data-breach