COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 2. February 06, 2020 Privacy Briefs: February 2020

By Jane Anderson

◆ **A ruling from Georgia's highest state court could set a precedent that determines recourse for victims of cyberattacks.**[1] The Georgia Supreme Court ruled in late December that the victims of a hack involving Athens Orthopedic Clinic can sue the clinic. The unanimous ruling reverses the Georgia Court of Appeals decision to throw the case out. The Georgia high court justices found that even the threat of future harm to a data breach victim is enough to warrant compensation under the law. This could set statewide precedent in these types of crimes. The hack involved a cybercriminal group calling itself the "Dark Overlord," and led to the breach of protected health information (PHI) for an estimated 200,000 patients. Athens Orthopedic Clinic refused to pay the hackers' ransom, and advised current and former patients to set up anti-fraud protections. Three patients sued, demanding that the clinic pay damages. The case now returns to the lower court in Athens-Clarke County for further proceedings.

◆ **In another lawsuit involving a data breach,**[2] **a Poughkeepsie, New York, woman has filed a class action suit in the U.S. District Court over a July 2018 phishing attack that exposed the personal and medical information of more than 28,000 customers of Health Quest**, a hospital and provider group. The lawsuit assailed the defendants "for their failure to exercise reasonable care in securing and safeguarding their patients' sensitive personal data," including names, dates of birth, Social Security numbers, driver's license numbers and financial account information. "Defendants' security failures enabled the hackers to steal the private information of plaintiff and members of the class.... These failures put plaintiff's and class members' private information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses," the lawsuit claims. Health Quest became part of Nuvance Health in a 2019 merger, and Nuvance also is named in the lawsuit.

◆ **A Richmond Hill, Georgia, man who claimed to be a whistleblower has been charged in federal court with falsely accusing a former acquaintance of patient privacy violations.**[3] According to a news release, "Jeffrey Parker, 43, is charged in a federal information with one count of False Statements," said Bobby L. Christine, U.S. Attorney for the Southern District of Georgia. The charge carries a possible sentence of up to five years in prison. Court documents indicate Parker "engaged in an intricate scheme" in which he contacted the U.S. Department of Justice (DOJ) to claim that a former acquaintance had violated HIPAA privacy provisions. As part of the alleged scheme, Parker created email addresses using the names of real individuals and pretended to be those individuals to make it appear as if his acquaintance had committed a crime. He sent those communications to the hospital where the acquaintance worked, to the DOJ, and to the FBI. Parker then claimed to have received threatening messages in retaliation for blowing the whistle, and FBI agents took steps to ensure his safety and quickly investigate the alleged crime. After an FBI agent interviewing Parker found inconsistencies in his story, Parker admitted the statements he made and emails he sent were false. "The allegations against Parker are disturbing because they not only undermine whistleblower laws, they also waste investigative resources and damage the falsely accused," said Chris Hacker, special agent in charge of FBI Atlanta. "Hopefully the quick uncovering of this alleged scheme by our investigators will send a message that these types of actions will be exposed and justice will be served."

◆ **Security firm vpnMentor says it discovered a data breach in THSuite, a point-of-sale system used in the**

cannabis industry.[4] The team, led by internet privacy researchers Noam Rotem and Ran Locar, identified an unsecured Amazon S3 bucket owned by THSuite that exposed sensitive data from multiple marijuana dispensaries and their customers around the U.S. The leaked data included scanned government and employee IDs, which exposed personally identifiable information for more than 30,000 individuals. The breach was discovered on Dec. 24, and the THSuite owners were contacted on Dec. 26, vpnMentor says. Amazon was contacted on Jan. 7, and the database was closed Jan. 14. Cannabis dispensaries need to collect large quantities of sensitive information in order to comply with state laws. According to the report, "In the sample of entries we checked, we found information related to three marijuana dispensaries around the U.S.: Amedicanna Dispensary, Bloom Medicinals and Colorado Grow Company." However, the researchers say the breach affected many more dispensaries.

◆ **Adventist Health says one of its hospitals in southern California experienced a phishing incident that compromised a worker's email account.**[5] Adventist Health Simi Valley said that the phishing incident occurred on Sept. 30, but officials did not discover that patient information was present in the worker's email account until Oct. 14. Patient information that may have been available through the worker's login credentials includes names, dates of birth, medical record numbers, hospital account numbers, insurance information, and other information related to care received as patients. Approximately 3,701 individuals spread across three communities were affected and are being offered a year of free identity theft protection services. Adventist Health also said it will take additional steps to ensure the event is resolved and institute additional training and protocols to ensure future phishing attempts fail.

◆ **Alomere Health in Minnesota is notifying patients about a data breach that affected nearly 50,000 patients following a phishing attack in which a malicious actor gained access to two employee email accounts late last year.**[6] The first incident occurred between Oct. 31 and Nov. 1, and the second one occurred on Nov. 6, according to Alomere Health. Working with a computer forensic firm, Alomere was unable to determine whether attackers actually viewed any email or attachments in any of the accounts. Alomere determined that portions of some patients' information were contained in the email accounts, such as patient names, addresses, dates of birth, medical record numbers, health insurance information, treatment information and diagnosis information. For a limited number of patients, Social Security numbers and/or driver's license numbers were found in the accounts. Alomere is offering free credit monitoring and identity protection services for the 694 patients whose Social Security numbers and/or driver's license numbers were contained in the email accounts.

◆ **Buck, an integrated human resources and benefits consulting firm, found in a survey on HIPAA readiness**[7] **that organizations are not fully compliant with HIPAA rules, nor are they prepared to undergo a HIPAA audit.** The survey found that 42% of participants did not know when a risk/threat analysis last was conducted, or last conducted such an analysis more than five years ago; 33% of respondents either have not inventoried their business associates or did not know if they have done so; 16% did not have current business associate agreements, or did not know if they had them; 35% indicated they last offered HIPAA training between one and five years ago; 13% provide training only during onboarding; and 10% did not know when HIPAA training last was provided. Buck surveyed companies across a wide range of industries, most of which were sponsors of group health plans.

◆ **SouthEast Eye Specialists Group, based in Franklin, Tennessee, is notifying around 13,000 patients that their PHI may have been exposed in a data breach during a phishing attack.**[8] The provider group noticed potentially suspicious activity on Nov. 1, and its information technology staff began an investigation, engaging computer forensic experts to determine if any information was affected. After examining the accounts, the investigation determined that personal information, possibly including Social Security numbers and treatment information, may have been contained in an affected email account. There is no indication that an unauthorized party

accessed or viewed patient information, and no evidence of patient information being misused, the provider group says.

◆ **The former director of a New Jersey EMS squad has filed a lawsuit against the town where he worked, alleging a series of hostile and unethical actions by one of his former supervisors, including HIPAA violations.**[9] Former Spotswood EMS director and EMT David Nichols said he faced "civil rights violations, harassment and retaliation" from administrator Dawn McDonald and was forced to resign his post in April 2019. Among Nichols' claims are that McDonald spread defamatory claims about him, that McDonald used security cameras to spy on him, and that McDonald asked him for access to confidential patient records and got access from someone else when he refused. McDonald was placed on administrative leave and investigated for claims made by Nichols in July 2019, but the town at the time found "no evidence of harassment, retaliation, discrimination or defamation." The borough of Spotswood and McDonald are named as defendants in the lawsuit, as is Spotswood Mayor Ed Seely.

1 Ben Brasch, "Ga. high court's ruling on 200K-victim cyber attack could set precedent," *The Atlanta Journal-Constitution*, December 25, 2019, https://bit.ly/2tKOhyf.
2 John W. Barry, "Data breach: Health Quest, Nuvance target of federal lawsuit," *Poughkeepsie Journal*, January 23, 2020, https://bit.ly/3aBhjRu.
3 Department of Justice, U.S. Attorney's Office for the Southern District of Georgia, "Richmond Hill man charged in 'intricate scheme' to frame former acquaintance in health care investigation," news release, January 8, 2020, https://bit.ly/3aG6Jsk.
4 vpnMentor, "Report: Cannabis Users' Sensitive Data Exposed in Data Breach," January 24, 2020, https://bit.ly/2vi6DqQ.
5 Staff Reports, "Adventist Health issues statement on email security incident," *The Sentinel*, January 17, 2020, https://bit.ly/2Gja82p.
6 Al Edenloff, "Alomere Health reports unauthorized access to emails," *Echo Press*, January 6, 2020, https://bit.ly/2RJ1LTg.
7 Buck, *2019 HIPAA Readiness Survey* , January 2020, https://bit.ly/38wplcD.
8 SouthEast Eye Specialists, "SEES Group Notifies Patients of Data Security Incident," https://bit.ly/2NRascL.
9 Carly Baldwin, "Former Spotswood EMT Sues Town, Alleging Hostile Work Environment," *Patch*, January 14, 2020, https://bit.ly/2NTWXcx.