San Francisco Chronicle

Lawsuit filed against 49ers over ransomware attack that hacked identities of 20,000

Sam Whiting

Sep. 11, 2022

Brandon Aiyuk (11) with a run after the catch in the third quarter as the San Francisco 49ers played the Los Angeles Rams in the NFL Championship game at SoFi Stadium in Inglewood on Jan. 30. Two weeks after the game, which the 49ers lost, the team issued a statement that their corporate IT network systems had been disrupted by a "network security incident," the Associated Press reported. Carlos Avila Gonzalez/The Chronicle

A ransomware attack during Super Bowl week on San Francisco 49ers systems that breached nearly 21,000 individual ticket-holder and vendor and employee files has resulted in a class action lawsuit filed Friday against the organization.

The suit, filed in Santa Clara County Superior Court by the Oakland firm Cole & Van Note, alleges invasion of privacy and negligence, breach of implied contract, unfair business practice and unjust enrichment by the 49ers Football Co.

The suit seeks an injunction to ensure that the company secures and sequesters cyberdata more effectively than before, along with unspecified damages. The lead plaintiff, John Garvey of Moraga, is a former security guard who received a letter from the 49ers in late August acknowledging that his name, date of birth and Social Security number had been taken in a cyberattack, said Scott Cole, lead attorney in the case.

“Mr. Garvey is gravely concerned that his identity has entered the hands of criminals and that he may never know the full extent of how the breach impacts him,” Cole said.

A 49ers team representative did not immediately respond Sunday to a request for comment.

Last week, the 49ers acknowledged that a ransomware attack during Super Bowl week, which had compromised its systems, had affected 20,930 individuals who may be victims of identity theft, according to a government notification filed by the team.

The 49ers issued a statement on Super Bowl Sunday, Feb. 13, that their corporate IT network systems had been disrupted by a “network security incident,” the Associated Press reported. The 49ers two weeks earlier had lost the NFC Championship Game to the L.A. Rams, who went on to win the Super Bowl.

The team took immediate steps to stop the access and enlisted an outside cybersecurity firm to investigate, according to a 49ers statement. The investigation was completed in August and found unauthorized access to files during the week of Feb. 6-11.

“We have begun notifying individuals whose data may have been compromised during a cybersecurity incident on our corporate network earlier this year and are offering complimentary credit monitoring and identity theft protection

services to them," Jacob Fill, 49ers corporate communications coordinator, said in response to a Chronicle query.

"We take seriously our responsibility to safeguard personal and sensitive information entrusted to us and are committed to working with cybersecurity experts to ensure we are protected from any future similar incidents. We regret any concern this has caused to the affected individuals."

The AP reported in February that the BlackByte ransomware gang had stolen some of the 49ers' financial data and posted it online, though the group did not make its ransom demands public or say how much data it had stolen or encrypted.

At the time, the team said in a statement that "we have no indication that this incident involves systems outside of our corporate network, such as those connected to Levi's Stadium operations or ticket holders," according to the AP.

However, in a subsequent filing with the Attorney General's Office in Maine — where reporting data breaches is mandatory, according to the Record, a cybersecurity news publication that first reported the 49ers breach notifications — 49ers outside counsel Jennifer Costa said 20,930 people may have been affected by the security breach. Social Security numbers were apparently taken. Seven of them are Maine residents, who were notified Sept. 1.

Costa, who works at the firm Baker & Hostetler in Cleveland, did not immediately respond to a request for comment Sunday.

Cole & Van Note specializes in cybersecurity cases, and Cole said this case could be deeply troubling because of the scope of the information taken, including sensitive employee data going back to the Candlestick era. The Cole & Van Note website has a portal for joining the case. "We take cyberbreaches like this seriously," Cole said. "We will know a lot more as documents and forensic reports come to light."

Sam Whiting is a San Francisco Chronicle staff writer.
Email: swhiting@sfchronicle.com