Fraud Management & Cybercrime , Healthcare , HIPAA/HITECH

5 Lawsuits Filed in Ransomware Breach Affecting 3.3 Million

Proposed Class Actions Against Regal Medical Group Allege Negligence, Other Claims

Marianne Kolbasuk McGee (HealthInfoSec) • February 22, 2023

Regal Medical Group in California is facing at least five proposed class action lawsuits following a ransomware incident involving data exfiltration that affected more than 3.3 million individuals.

At least five proposed class action lawsuits have been filed in recent days in the wake of a California medical group's Feb. 1 report of a ransomware attack last December that affected more than 3.3 million individuals.

See Also: OnDemand | Navigating the Difficulties of Patching OT

The proposed lawsuits filed so far against Regal Medical Group, its affiliated Heritage Provider Network and other affiliated groups include four federal complaints filed since Feb. 13 in the U.S. District Court for the Central District of California, plus at least one complaint filed in a California state court on Feb. 9.

Regal, which has more than 3,000 doctors and touts itself as one of the largest physician-led healthcare networks in southern California, reported the hacking incident on Feb. 1 to the Department of Health and Human Services as affecting several of its affiliated medical groups.

The groups whose patients were affected by the incident include Lakeside Medical Organization and Affiliated Doctors of Orange County and Greater Covina Medical Group. The groups also are affiliates of Heritage Provider Network, a managed care plan (see: *California Medical Group's Ransomware Breach Afects 3.3M*).

"It is astonishing that these multiple affiliated organizations, which held the data of over 3.3 million individuals, would not have taken their cybersecurity obligations more seriously," says attorney Scott Edward Cole of the law firm Cole & Van Note, which is representing plaintiffs in a lawsuit filed in California superior state court against Regal, Heritage and their other affiliated medical groups.

"The information accessed here was the Holy Grail of health and financial data, the kinds of information extraordinarily valuable to criminals," Cole tells Information Security Media Group.

Attorney Brian Gudmundson, a partner at Zimmerman Reed LLP, which is representing plaintiffs in one of the lawsuits filed in federal court, says he and his legal team are looking forward to pursuing their clients' claims and the rights of all of the victims of this "preventable" breach.

"We are very concerned by both the incredible scope of victims in this data breach … and the extremely sensitive data taken, which allegedly includes Social Security numbers and healthcare information," Gudmundson says.

Regal and Heritage declined ISMG's requests for comment on the pending litigation.

Lawsuit Allegations

Each of the lawsuits seeks class action certification and makes similar claims against Regal.

The claims include allegations that the organization was negligent in failing to secure individuals' sensitive health information; that the entity violated various state and federal laws, including California privacy, consumer and unfair business laws, and also HIPAA and the Federal Trade Commission Act; and that the incident has put plaintiffs and class members at significant risk of harm, including identity theft and fraud.

"Despite knowing the prevalence of data breaches, Regal Medical Group failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases," alleges the federal lawsuit complaint filed on Feb. 16 by plaintiff David Rodriguez on behalf of himself and others similarly situated.

"Regal Medical Group has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches," the lawsuit alleges. Among other things, it says, Regal failed to adequately analyze and test its own systems, train its own personnel and take other data security measures to ensure that vulnerabilities were avoided or remedied and that the plaintiff's and class members' data was protected.

Relief sought by the various lawsuits includes actual and punitive damages and permanent injunctive relief to prohibit Regal from engaging in "unlawful acts, omissions, and practices" as described in the complaints.

Breach Details

In its breach notice, Regal says that on Dec. 2, 2022, employees noticed difficulty in accessing some of the organization's servers.

After an "extensive" review, malware was detected on some of Regal's servers, which a threat actor used to access and exfiltrate data, the notice says. Regal became aware of the breach on Dec. 8, and the breach was determined to have occurred "on or about Dec. 1," the notice says.

Patient data potentially compromised in the incident includes names, Social Security numbers, addresses, birthdates, diagnosis and treatment information, laboratory test results, prescription data, radiology reports, health plan member numbers and phone numbers.

The organization is offering affected individuals one year of complimentary credit monitoring and says it notified law enforcement about the incident.

As of Wednesday, the Regal breach was by far the largest posted so far in 2023 to the HHS Office for Civil Rights' HIPAA Breach Reporting Tool website listing health data breaches affecting 500 or more individuals. Regal reported the breach to HHS OCR as a hacking incident involving a network server.