Union sues feds over hack, says agency had ample warning

June 30 2015, byKen Dilanian

In this June 25, 2015 file photo, Office of Personnel Management (OPM) Director Katherine Archuleta testifies on Capitol Hill in Washington. The federal personnel agency whose records were plundered by hackers linked to China says it has temporarily shut down a massive database used to update and store background investigation records. The agency says a newly discovered flaw left the system vulnerable to hackers. (AP Photo/Susan Walsh)

The largest federal employee union filed a class action lawsuit Monday

against the federal personnel office, its leaders and one of its contractors, arguing that negligence contributed to what government officials are calling one of the most damaging cyberthefts in U.S. history.

The suit by the American Federation of Government Employees names the Office of Personnel Management, its director, Katherine Archuleta, and its chief information officer, Donna Seymour. It also names Keypoint Government Solutions, an OPM contractor.

Hackers suspected of working for the Chinese government are believed to have stolen records for as many as 18 million current and former federal employees and contractors last year. Detailed background investigations for security clearances of military and intelligence agency employees were among the documents taken.

OPM acknowledged the hack earlier this month, and has come under withering criticism from lawmakers and outside experts ever since. The agency's inspector general told Congress he had been warning for years that the agency's information security was inadequate but those warnings went largely unheeded.

The lawsuit alleges that OPM was negligent when it failed to improve its security and safeguard employee information despite the warnings. The suit says an earlier hack of Keypoint systems allowed the attackers to obtain credentials that led to the later breaches.

"Since 2007, officials at OPM have been alerted to their lackluster data security policies and protocols and failed to take appropriate steps to safeguard the information," AFGE National President J. David Cox Sr. and other union officials said in a joint statement. "Although they were forewarned about the potential catastrophe that government employees faced, OPM's data security got worse rather than better."

The suit seeks unspecified monetary damages and calls for more extensive credit monitoring for employees who had their personal information stolen, saying the 18 months of monitoring offered by OPM is inadequate.

"We want the OPM and other responsible parties to take responsibility, do everything feasible to remedy the problem and ensure that our clients do not suffer any further harm as a result of their information being compromised," said Daniel Gerard, the lawyer representing the union.

OPM and Keypoint did not immediately respond to requests for comment.

The suit came on the same day that OPM said it has shut down a massive database used to update and store background investigation records after discovering a new flaw that left the system vulnerable to additional breaches.

The database is known as e-QIP, short for Electronic Questionnaires for Investigations Processing.

There is no evidence the vulnerability has been exploited by hackers, agency spokesman Samuel Schumach said in a statement, adding that OPM took the step protectively after analyzing its networks for security flaws. He said the system could be shut down for four to six weeks.

The shutdown is expected to hamper agencies' ability to initiate investigations for new employees and contractors, as well as renewal investigations for security clearances, Schumach said.

But, he added, the federal government will still be able to hire, and in some cases grant clearances on an interim basis.