DC Appeals Court Green-Lights Data Breach Lawsuit Against Office of Personnel Management

June 21, 2019 - The federal appeals court for the District of Columbia overturned a lower court ruling today that was preventing a data breach case filed by federal employees against the Office of Personnel Management (OPM). The 2014 breach impacted 22 million federal employees and contractors and has been widely blamed for a large number of identity theft and fraud cases. The breach also included vetting data used by the government for security clearances, as well as biometric data on those currently possessing such clearances.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

OPM was clearly culpable in the breach. The agencies own Inspector General was so alarmed with the state of data security at OPM that he had advised the agency to shut its computer network down. While that request was made prior to the data breach being discovered, hackers had already penetrated the network. It is believed that the Chinese government was responsible; meaning that the breach also damaged national security.

The lower court ruling throwing the case out stated that there was no proof the breach had resulted in identity theft and therefore the plaintiffs didn't have standing to sue. But the appeals court disagreed. In the new ruling, the court said that there was no doubt that the breach left victims vulnerable to identity theft and that the threat was ongoing and significant. The court said that this alone amounted to an "injury" for the plaintiffs, giving them standing the sue. In a review of the types of data stolen, the court wrote, "It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft."

The appeals court also leveled significant criticism at the district court for using outside sources of information to reach a determination that the attack posed little threat of identity theft to victims. Those outside reports led the court to conclude that the Chinese government was behind the attack and that its motives had nothing to do with identity theft.

But the appeals court points out in its ruling that there is nothing to say that espionage on the part of China wouldn't include the use of identity theft as a weapon against us. And we believe that the court might be right. After all, if you could steal the identities of those with security clearances and ruin their credit, that would force the government to rescind those clearances and could create havoc in a variety of sensitive professions.

Perhaps the most important finding of the court was a conclusion that even four years after the breach occurred, OPM

has still failed to secure its computer systems. Fortunately, after the breach congress moved responsibility for new background checks from OPM to the Pentagon. The Trump administration is now threatening to close OPM down by the end of October due ty lack of funding from congress.

The case will now go back to the district court and be allowed to move forward.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS