

House: Private laptop theft from US hits 'most vulnerable'

April 5 2016, by Jack Gillum



In this Dec. 17, 2015 file photo, Rep. Jason Chaffetz, R-Utah speaks on Capitol Hill in Washington. Chaffetz, chairman of the House Oversight and Government Reform Committee, demanded to know Tuesday, April 5, 2016, why a personal laptop taken from a federal building in Washington state was used to conduct child-support audits, especially because it and stolen hard drives may have contained millions of names and Social Security numbers. (AP Photo/J. Scott Applewhite, File)

The top watchdogs in the House demanded to know Tuesday why a personal laptop taken from a federal building in Washington state was used to conduct child-support audits, especially because it and other stolen hard drives may have contained millions of names and Social Security numbers.

The letter by the House government oversight panel's Republican chairman and senior Democrat to Health and Human Services Secretary Sylvia Burwell comes about a week after GOP investigators began looking into the breach in Olympia, Washington, which authorities say affected as many as five million people.

"Your staff acknowledged that the use of personal equipment is a clear violation of HHS privacy and security policy," Utah Republican Jason Chaffetz and Maryland Democrat Elijah Cummings wrote in the letter obtained by The Associated Press. The break-ins occurred in early February at the federal Office of Child Support Enforcement.

Chaffetz's committee has been critical of data breaches under the Obama administration, including when the U.S. Office of Personnel Management said last year hackers committed an unprecedented theft of private data for millions of federal workers.

The letter comes a day after Chaffetz's counterpart in the Senate, Republican Sen. Ron Johnson of Wisconsin, sent a similar message to Burwell asking what specific information was on the hard drives, when officials first became aware of the burglaries and if the government will notify those whose data were stolen.

But Chaffetz and Cummings also questioned why HHS officials waited nearly two months to provide Congress with notification under the Federal Information Security Management Act, which they said requires notice no later than a week after a major incident took place. They also

asked what databases could have been accessed.

"HHS hasn't been forthcoming about this incident, so it's unclear who or what is at risk," Chaffetz said in a statement Tuesday to the AP. "As we experienced with OPM, this administration initially downplayed the extent of the breach," adding the possibility that a "significant amount" of personally identifiable information could have been compromised for "our most vulnerable children and families."

In addition to 4.2 million people whose records were stolen in the initial OPM hack, more than 21.5 million had their Social Security numbers and other sensitive information stolen in a second breach, believed to be the biggest in U.S. history. OPM later offered credit-monitoring services and identity-theft insurance to those affected.

An HHS spokeswoman acknowledged late Monday that the stolen equipment in Olympia may have contained personal information, adding the incident was a property theft and not an intrusion of federal networks.

Court documents showed the stolen hard drives had between 2 million and 5 million individual profiles containing names, Social Security numbers, birthdates, addresses and phone numbers, according to federal investigators.

Police said the intruders used a copy of a building key kept by a former building employee, who was ultimately fired for stealing. Court records stated she was arrested recently in connection with the burglaries.

The Office of Child Support Enforcement oversees child-support programs across the nation. One suspect told police he was inside the building for two hours during the burglary, when \$600 in cash and a government credit card were also taken.

"If the hard drives are accessed, there would be a large data breach," Thurston County, Washington, prosecutors said in court filings last week. It was unclear if the drives were encrypted, which would make it harder for thieves to copy data.

Olympia police said they've arrested two in connection with the thefts, including 28-year-old Nicholas Perring, who was charged with second-degree burglary and had bail set at \$10,000. The other, Demario Heard, was also arrested on suspicion of meth possession.

Perring told investigators he and Heard split the \$600, found in a bag, to go gambling. Police later reported camera equipment missing from a separate Federal Highway Administration office in the building, as well as Super Mario Bros. and Legend of Zelda video games from a nearby business.

The Federal Protective Service declined to comment on the case, citing an ongoing investigation.

© 2016 The Associated Press. All rights reserved.

Citation: House: Private laptop theft from US hits 'most vulnerable' (2016, April 5) retrieved 25 June 2024 from <https://phys.org/news/2016-04-house-private-laptop-theft-vulnerable.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.