Health data breach hitting Congress 'could be extraordinary'

March 9 2023, by LISA MASCARO and FRANK BAJAK

People walk outside the U.S. Capitol building in Washington on June 9, 2022. Members of the House and Senate were informed Wednesday, March 8, 2023, that hackers may have gained access to their sensitive personal data in a breach of a Washington, D.C., health insurance marketplace. Credit: AP Photo/Patrick Semansky, File

House leaders say the impact of a hack of a health insurance marketplace used by members of Congress "could be extraordinary," exposing sensitive personal data of lawmakers, their employees and families. In all, thousands of people could be affected.

DC Health Link, which runs the exchange, said an unspecified number of customers were impacted and it was notifying them and working with law enforcement to quantify the damage. It said it was offering identity theft service to those affected and extending credit monitoring to all customers.

Some 11,000 of the exchange's more than 100,000 participants work in the House and Senate—in the nation's capital and district offices across the nation—or are relatives.

In a letter to the exchange's director posted on Twitter, House Speaker Kevin McCarthy, R-Calif., and Minority Leader Hakeem Jeffries, D-N.Y., said the breach "significantly increase the risk that Members, staff and their families will experience identity theft, financial crimes, and physical threats." The stolen data includes Social Security numbers, phones, addresses, emails and employer names.

The FBI said in a brief statement Wednesday evening it was aware of the incident and was assisting.

In the letter, McCarthy and Jeffries said the FBI had not yet determined the extent of the breach but that thousands of House members, employees and their families have enrolled in health insurance through DC Health Link since 2014. "The size and scope of impacted House customers could be extraordinary."

They said the FBI told them it was able to purchase the stolen data on the dark web, where it was offered for sale for an unspecified amount

Monday on a hacker forum popular with cybercriminals.

It was not clear, though, whether and how the FBI could guarantee that copies of the stolen data were not circulating in the cybercrime underworld. Indeed, on Thursday, a new user on the forum claimed a hacker known as "thekilob" had stolen more than 55,000 records and exclaimed "Glory to Russia" in Cyrillic. Some of the most active cybercriminals are Russian speakers and operate with little interference from the Kremlin.

The user posted 200 records from the hack online and The Associated Press confirmed the sample's authenticity with two of the victims listed.

"This is big. This isn't just like regular folks. This is everyone," said one victim who works in Washington, D.C. In all, 24 people in her office had their records in the dump. The AP is not naming victims or their workplaces to avoid further potential harm.

Sample data posted to the hacker forum by a different account—and removed overnight Thursday—listed data for a dozen DC Link participants. The AP reached one by phone.

"Oh my God," the man said, when informed the information was public. All 12 people listed work for the same company or are family members.

In an email to all Senate email account holders on Wednesday, the sergeant at arms recommended that anyone registered on the health insurance exchange freeze their credit to prevent identity theft.

An email sent out by the office of the Chief Administrative Office of the House on behalf of McCarthy and Jeffries called the breach "egregious" and urged members to use credit and identity theft monitoring resources.

In an emailed statement on Wednesday, Rep. Joe Morelle of New York said House leadership was informed by Capitol Police that DC Health Link "suffered an extraordinarily large data breach of enrollee information" that posed a "great risk" to members, employees and their family members. He said the FBI was still determining the "cause, size, and scope of the data breach."

The hack follows several recent breaches affecting U.S. agencies. Hackers broke into a U.S. Marshals Service computer system and activated ransomware on Feb. 17 after stealing personally identifiable data about agency employees and targets of investigations.

An FBI computer system was recently breached at the bureau's New York field office, CNN reported in mid-February. Asked about that intrusion, the FBI issued a statement calling it "an isolated incident that has been contained." It declined further comment, including when it occurred and whether ransomware was involved.

There was no indication the DC Health breach was ransomware-related.