MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

June 21, 2018

The Honorable Jeff Sessions
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Jeff T.H. Pon
Director
U.S. Office of Personnel Management
1900 E Street, NW
Washington, DC 20415

Dear Attorney General Sessions and Director Pon:

According to a Monday press release from the Department of Justice, an individual pleaded guilty to using the stolen personal identifying information of victims of the 2015 Office of Personnel Management hack in a *domestic* case of fraud. All prior public information was that this data breach was caused by Chinese hackers, yet, according to the DOJ, this information is now in the hands of U.S. residents for illicit use, and may have been as early as 2015. Despite my staff reaching out, I have not received any additional information from either of your offices on how this fraud is connected to the 2015 OPM data breach, nor has there been any public alert that those subject to the breach may be at greater risk to domestic fraud.

This is unacceptable, and DOJ and OPM need to provide more information about whether millions of current and former federal employees are at risk of their personal information being used for fraudulent purposes here in the U.S., or around the world.

In 2015, the personal identifying information – including detailed information from government background investigations – for more than 21 million current and former federal workers was compromised. The federal government was too slow in notifying the public about what happened, and too slow in taking steps to assist federal workers whose information was hacked. After significant pressure from my office and a number of my colleagues in the Senate, OPM finally took the right steps to assist federal workers subject to the hack.

It seemed that OPM got the message on the seriousness of this issue, and that federal agencies would be proactive in keeping the public up-to-date on what happened and the risks they face. But events in the last few days now put this in question.

Since 2015, the public information from the federal government has been that these breaches likely originated from Chinese hackers – not cyber criminals – and that there was not a risk of domestic use of this information for criminal or fraudulent purposes.

However, Monday's announcement that a U.S. resident used the private information of OPM data breach victims to fraudulently acquire loans in Virginia calls this assumption into question.

Efforts by my office to get additional information on how this case is connected to the 2015 OPM breach have been unsuccessful; neither OPM nor the DOJ has been forthcoming with any additional information than that which was included in the public press statement.

I expect that you will follow up with my office about what happened and the potential risk for the millions of Americans who had their information stolen. My staffer, Jonathan Goldman, should be your point of contact, and can be reached at Jonathan_Goldman@warner.senate.gov. I expect to hear answers no later than Wednesday June 27th. Our current and former federal workers deserve answers.

Sincerely,

Mark R Warner

MARK R. WARNER
United States Senator