CAROLYN B. MALONEY
CHAIRWOMAN

ONE HUNDRED SIXTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

JAMES COMER
RANKING MINORITY MEMBER

October 20, 2020

The Honorable Robert Wilkie
Secretary
Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, D.C. 20420

Dear Secretary Wilkie:

The House Committee on Oversight and Reform Republicans are conducting oversight of a recent data breach at the U.S. Department of Veterans Affairs (VA). On September 14, 2020, the VA announced a data breach involving the personal information of 46,000 veterans.[1] Specifically, unauthorized users recently compromised an online application used to process payments to community health care providers for medical treatment of veterans. As such, we are writing to request more information on how the VA is protecting the personal information of veterans.

The VA's investigation thus far indicates that unauthorized users gained access through social engineering techniques and by exploiting authentication protocols to change financial information and divert payments from the VA that were intended to reimburse community health care providers.[2] Apparently, these unauthorized users were also able to access personally identifiable information of veterans receiving care from community health care providers, including social security numbers.

Upon discovering the data breach, the VA appears to have immediately initiated an investigation, took the application offline, and made a public announcement. The VA is also alerting affected individuals of the potential risk to their personal information through a letter mailer and is offering free credit monitoring services to individuals whose social security numbers were compromised.[3]

---

[1] Press Release, U.S. Department of Veterans Affairs, *VA notifies Veterans of compromised personal information* Sept. 14, 2020, *available at* https://www.va.gov/opa/pressrel/pressrelease.cfm?id=5519#:~:text=WASHINGTON%20%E2%80%94%20The%20U.S.%20Department%20of,potential%20harm%20to%20those%20individuals.
[2] *Id.*
[3] *Id.*

Although we commend the VA for its apparent quick response in taking the application offline and investigating the breach, as well as its efforts to notify affected individuals, we are concerned about veterans' personal information being vulnerable and the potential consequences data breaches such as this have on affected veterans.

This issue is not unique to the VA's online applications. A recent investigation by the VA Office of Inspector General (OIG) found that some veterans' sensitive personal information was left unprotected on shared network drives, potentially accessible by Veterans Service Organization officers who did not represent those veterans and had no need for such information.[4] Although no known data breaches occurred as a result, the VA did concur with all the OIG's recommendations and implemented a corrective action plan.[5]

Data breaches of any kind are concerning, but particularly so when the targeted data is held in trust by the U.S. Government and where it affects veterans. To that end, we request a staff-level briefing by the VA sufficient to answer the following questions:

1. When did the VA become aware of the data breach and what steps were taken to secure the affected application?

2. How many unauthorized users were identified by the VA on the payment processing application?

3. How long were veterans' personal information potentially exposed to unauthorized users on the affected application?

4. How did the VA determine the 46,000 veterans who were potentially affected and how are notifications being made to those veterans?

5. What are the potential negative consequences for a veteran whose information was compromised in the breach?

6. What steps is the VA taking to ensure that veterans' personally identifiable information remains secure on VA data networks as well as VA online applications?

This briefing may be conducted remotely for convenience. To schedule the briefing or ask any follow-up or related questions, please contact Committee on Oversight and Reform staff at (202) 225-5074.

---

[4] U.S. Department of Veterans Affairs Office of Inspector General, *Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives*, Report 19-06125-218, Oct. 17, 2019, *available at* https://www.va.gov/oig/pubs/VAOIG-19-06125-218.pdf

[5] *Id.*

The Committee on Oversight and Reform is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. Thank you in advance for your cooperation with this inquiry.

Sincerely,

Jody Hice
Ranking Member
Subcommittee on Government Operations

James Comer
Ranking Member
Committee on Oversight and Reform

Glenn S. Grothman
Ranking Member
Subcommittee on National Security

Michael Cloud
Ranking Member
Subcommittee on Economic and Consumer Policy

Chip Roy
Ranking Member
Subcommittee on Civil Rights and Civil Liberties

Mark E. Green, M.D.
Ranking Member
Subcommittee on Environment

Paul A. Gosar, D.D.S.
Member of Congress

Virginia A. Foxx
Member of Congress

Clay Higgins
Member of Congress

Ralph W. Norman
Member of Congress

Carol D. Miller
Member of Congress

W. Gregory Steube
Member of Congress

Fred B. Keller
Member of Congress

cc: The Honorable Carolyn Maloney, Chairwoman
Committee on Oversight and Reform

The Honorable Gerald E. Connolly, Chairman
Subcommittee on Government Operations

The Honorable Stephen F. Lynch, Chairman
Subcommittee on National Security

The Honorable Raja Krishnamoorthi, Chairman
Subcommittee on Economic and Consumer Policy

The Honorable Jamie Raskin, Chairman
Subcommittee on Civil Rights and Civil Liberties

The Honorable Harley E. Rouda, Chairman
Subcommittee on Environment