CAO
CHIEF ADMINISTRATIVE OFFICER

***Correction:** To speak with a representative from Experian, please call the updated number below.*

Dear Colleague,

I have been informed by the United States Capitol Police and DC Health Link* of a data breach impacting Members and staff. DC Health Link suffered a significant data breach yesterday potentially exposing the Personal Identifiable Information (PII) of thousands of enrollees. As a Member or employee eligible for health insurance through the DC Health Link, your data may have been comprised.

Currently, I do not know the size and scope of the breach, but have been informed by the Federal Bureau of Investigation (FBI) that account information and PII of hundreds of Member and House staff were stolen. I expect to have access to the list of impacted enrollees later today and will notify you directly if your information was compromised. DC Health Link will also likely contact you.

It is important to note that at this time, it does not appear that Members or the House of Representatives were the specific target of the attack.

While we do not yet know whether other enrollees have been compromised, out of abundance of caution you may wish to freeze your family's credit at the three major credit bureaus:

- **Call Equifax** at 800-349-9960 or freeze your credit online.
- **Call Experian** at 888-397-3742 or freeze your credit online.
- **Call TransUnion** at 888-909-8872 or freeze your credit online.

Freezing your credit is free and will not impact your credit score. A credit freeze keeps the personal information in your credit files from being accessed without your consent. It should prevent anyone, *including you,* from opening a credit card, or taking out a loan in your name. Please remember to write down the password you create as you freeze your credit as you will likely need to unfreeze it at some point in the future.

Please follow these step-by-step instructionsfor freezing your credit, and the additional steps you can take to avoid becoming a victim of identity fraud at the end of this message.

Speaker McCarthy and Democratic Leader Jeffries have formally requested additional information from DC Health Link on what data was taken, who was impacted, and what

steps they are taking – including providing credit monitoring protections – to protect House victims of this breach.

I will update you when I have more information.

Sincerely,

Catherine L. Szpindor
Chief Administrative Officer
U.S. House of Representatives

***The DC Health Exchange administers health care plans for Members and designated staff of Members, Committee and Leadership. Enrollees in health insurance through FEHBP are not affected by this incident.*

Additional Precautions to Help You Avoid Becoming a Victim of Financial Fraud

- Use two-factor authentication on all of your banking and utilities accounts and apps. The simple act of entering a code on your phone adds layers of protection to your accounts.
- Don’t click on links in emails, especially links that ask you to update personal information.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., ".com" vs. ".net").
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information.
- Do not reveal personal or financial information on the internet. Refer to these tips from Ready.gov.

- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at IC3.gov.
- Find additional information about preventative steps by consulting the Federal Trade Commission's website: Consumer.gov/IDTheft. The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below:
    - Identity Theft Clearinghouse
      Federal Trade Commission
      600 Pennsylvania Avenue, NW
      Washington, D.C. 20580
      Consumer.gov/IDTheft
      1-877-IDTHEFT (438-4338)

Member Focused. Service Driven.

Stay connected to the CAO and House community:

CAO Status (Snow) Line: 202-226-7669