Update #1 - Data Breach at DC Health Benefit Exchange Authority (HBX)

The Office of the Sergeant at Arms continues to work closely with the U.S. Capitol Police and other law enforcement organizations to determine the scope and scale of this data breach. Law enforcement provided the SAA with names of Senate employees whose PII was disclosed in this data breach. While it is the responsibility of HBX to contact these individuals, since we received the information from law enforcement, we reached out so those affected could begin to take proactive steps. If you did not receive a notice from **SOC@saa.senate.gov** indicating that you were impacted by this breach, then your name was not on the list we received from law enforcement.

We have additional information to share about the extent of the breach. The Personally Identifiable Information (PII) disclosed in the breach is extensive and includes: First Name, Last Name, SSN, DOB, Gender, Home Address, Mailing Address, Work Email, Home Email, Phone Number, Race, Ethnicity and Citizenship Status, as well as plan subscriber information for employees and their dependents.

If you have questions about your benefit status or benefits in general, please call the Disbursing Office Health Care Section at 202-224-8008 or the Employee Benefits Section at 202-224-1093.

Currently, we do not have information on the timeframe of data included in the breach, nor do we know if the list we received is all inclusive. We will continue to keep the community updated as we receive new information.

Recap of advice

- We highly recommend that you freeze your family's credit (including your children) at all three major credit bureaus. A credit freeze keeps the personal information in your credit file 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 keep track of the password you use for the credit freeze as you will need it to unfreeze your credit if you need to take out a loan in the future.

    - **Equifax** – Call 800-349-9960 or freeze your credit online: https://www.equifax.com/personal/credit-report-services/credit-freeze/
    - **Experian** – Call 800-397-3742 or freeze your credit online: https://www.experian.com/freeze/center.html
    - **TransUnion** – Call 888-909-8872 or freeze your credit online: https://www.transunion.com/credit-freeze

- Sign up for PrivacyBee at https://privacybee.com/ to have your personal data removed from data broker and junk mail sites. They will scan recent data breaches and evaluate your personal exposure.

- Placing a Fraud Alert on your credit is also a good idea, and that's done by calling one the three credit bureaus (above). The difference between a Freeze and Fraud Alert is outlined in a Federal Trade Commission (FTC) document under Additional Resources (below).
- We recommend that you request a copy of your credit report and check it to ensure it accurately reflects your accounts. You should do this again in a few months to keep tabs on open accounts in your name (see below).
- Use two-factor authentication on all your banking and utilities accounts and apps. The simple act of entering a code on your phone adds layers of protection to your accounts.
- Do not click on links in emails, especially links that ask you to update personal information.
- Pay attention to a website's URL. 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. See these tips from Ready.gov: https://www.ready.gov/cybersecurity#before.
- Take steps to monitor your PII and report any suspected instances of identity theft to the Federal Bureau of Investigation Internet Crime Complaint Center at http://www.ic3.gov.
- Additional information about preventative steps is available by consulting the Federal Trade Commission's website: http://www.consumer.gov/idtheft.

Additional Resources:

- Step-by-step instructions on freezing your credit: https://www.nerdwallet.com/article/finance/how-to-freeze-credit
- Information from the FTC on obtaining free credit reports: FTC.FreeCreditReports
- Information from the FTC on credit freezes and fraud alerts: https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts
- If someone has stolen your identity: https://www.identitytheft.gov/#/
- To dispute information on your credit report: https://www.experian.com/blogs/ask-experian/credit-education/faqs/how-to-dispute-credit-report-information/

The Senate Operations Center (SOC) and the SAA's cybersecurity team will continue to monitor the situation and keep the community updated. The SOC can be reached at 202-224-1800 or SOC@saa.senate.gov.

***Note:* If you have questions about your benefit status or benefits in general, please call the Disbursing Office Health Care Section at 202-224-8008 or the Employee Benefits Section at 202-224-1093.**