(December 11, 2015)

In order to further improve the lines of communication and to respond to the concerns between the National VA Council and you our members, I have established a National VA Council Briefing. This NVAC Briefing will bring you the latest news and developments within DVA and provide you with the current status of issues this Council is currently addressing. I believe that this NVAC Briefing will greatly enhance the way in which we communicate and the way in which we share new information, keeping you better informed.

Alma L. Lee
National VA Council, President

~~~~~~

In This Briefing: NEWS RELEASE: OPM Completes Initial Mailing of Notification Letters to Individuals Impacted by the Theft of Background Investigation Records

~~~~~~

FOR IMMEDIATE RELEASE
Friday, December 11, 2015

Contact: OPM Office of Communications
(202) 606-2402 or media@opm.gov

OPM Completes Initial Mailing of Notification Letters to Individuals Impacted by the Theft of Background Investigation Records

WASHINGTON, DC – The U.S. Office of Personnel Management (OPM), in partnership with the U.S. Department of Defense (DOD), has concluded the initial mailing of letters to roughly 93% of individuals whose Social Security Number and other personal information was stolen in the cyber incident relating to background investigation records. Additional letters will be mailed as individuals contact the verification center or if we can obtain better addresses for letters returned to sender through the postal service.

OPM has engaged in a rigorous process to notify impacted individuals through a method that prioritized the security of their information. Additionally, significant time and effort was spent to collect appropriate contact information for impacted individuals. To collect the addresses for individuals who could not be located, and to assist those who have issues with their PIN, the government established a verification center operated by DOD. The verification center will also serve as a resource for people who believe they may have been impacted, but have not yet received a letter.

The letters, examples of which can be found at www.opm.gov/cybersecurity, detail information on credit monitoring and identity theft protection services and insurance the U.S. Government is providing at no cost to the impacted individuals and their dependent minor children (under the age of 18 as of July 1, 2015) for a period of three years. Individuals can reach the verification center by going to www.opm.gov/cybersecurity and navigating to the "Verify If You Were Impacted" section. After contacting the verification center, people will receive a letter stating whether or not our records indicate that their Social Security Number was compromised in the intrusion. Due to security and privacy protections, this process may take a few weeks.

People who receive a letter should confirm that the letter matches those displayed on the OPM website. The letter should direct them to OPM's cybersecurity page at the address listed above. Any email that asks for personal information, or any version of the letter that does not direct individuals to OPM's cyber security website, should be considered fraudulent, and reported to local law enforcement, and the Federal Trade Commission (FTC) at https://www.ftccomplaintassistant.gov.

"OPM and our partners across government remain committed to protecting the safety and security of the information provided to us," **said OPM Press Secretary Sam Schumach**. "Together with our interagency partners, OPM is dedicated to delivering high-quality identity protection services to impacted individuals. The interagency team continues to review the impacted data to monitor for any misuse, and the U.S. Government will also continue to evaluate the coverage being provided and whether any adjustments are appropriate in association with this incident."

OPM has issued the following guidance to impacted individuals:

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax®, Experian®, and TransUnion® – for a total of three reports every year. Contact information for the credit bureaus can be found on the FTC website, www.ftc.gov.

- Review resources provided on the FTC identity theft website, www.ftc.gov/idtheft. The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.

How to avoid being a victim of fraud:

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).
- 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).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, http://www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007).
- Take advantage of any anti-phishing features offered by your email client and web browser.

The general public can obtain additional information about the steps they can take to avoid identity theft from the following agencies. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

For California Residents:
Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft

For Kentucky Residents:
Office of the Attorney General of Kentucky
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
Telephone: 1-502-696-5300

For Maryland Residents:
Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Telephone: 1-888-743-0023

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502

- end -