Security Breach Notification of Sailors' PII FAQ

"The Navy takes this incident very seriously - it is a matter of trust. That is why we are doing everything we can to take care of our current and former Sailors. It is important for them and their families to know we are working on their behalf when incidents like this occur."-- Chief of Naval Personnel Vice Adm. Robert Burke.

Q: What happened?
Oct. 27, 2016, a contractor notified Navy that it had detected activity indicating a contractor laptop being used to support a Navy contract may have been accessed without authorization. Following a careful review and analysis by both the contractor and Navy, it was determined on Nov. 22, 2016, that the names and Social Security Numbers of 134,386 current and former Sailors may have been accessed without authorization by an unknown actor.

Q: Who was affected?
Of the population whose information was stored on the laptop, 85,592 are active duty and 48,794 are civilians. 39,420 are Reserve Component members.

Q: What personal identifying information may have been compromised?
While we cannot conclusively determine any information was accessed or copied, the names and Social Security Numbers of the affected individuals were stored on the contractor laptop. Out of an abundance of caution and in keeping with our commitment to our Sailors, Navy is providing this notice and service.

Q: Has this information been misused in any way?
There is no evidence to suggest misuse of the information that was compromised.

Q: How will individuals find out if they were affected?
Navy has begun notifying those whose names and Social Security Numbers were stored on the affected laptop. Navy expects to have the notification process completed within the next several weeks.

Q: Why has it taken so long to notify affected Sailors?
We regret the delay that has occurred with your notification, and we take this potential data compromise very seriously – this is a matter of TRUST for our Sailors, both past and present. Navy sought to obtain services that would fully protect its Sailors should they be needed while at the same time following the rules and procedures intended to ensure the integrity of the procurement process.

Q: What type of credit monitoring protection will the Navy offer?
For those whose names and Social Security Numbers were stored on the affected laptop, Navy is providing a comprehensive suite of identity theft protection free of charge for up to three years beginning July 18, 2017, including:

- Full-service identity theft restoration, which helps to repair your identity following fraudulent activity since the date of the compromise
- Identity theft insurance, which can help reimburse you for certain expenses incurred if your identity is stolen since the date of the compromise
- Continuous identity and credit monitoring

Q: How does the credit services Navy is offering relate to other credit services offered to Government employees affected by previous breaches like the Office of Personnel Management breach?

The services are similar and if you have enrolled in similar services in the past because of other cyber incidents and breaches, including the 2015 cybersecurity incident at the Office of Personnel Management, you need take no further action at this time.

Q: I received a letter stating that I have been affected. What should I do next?
Please refer to the instructions in the letter. To register for these services, please visit: www.identityforce.com/navy. Each letter will provide a unique 25-digit pin number that individuals will need to be able to request credit monitoring services.

Q: How long will these services be available?
Navy is providing its Sailors credit monitoring, identity restoration services, and identity theft insurance coverage that will be available through July 18, 2020. Any identity theft claim during this period submitted by someone enrolled in this service will be investigated and worked until the affected individual's identity is restored.

Q: Will there be an information line if I have questions?
Yes. If you have questions, please email: N1Privacy.fct@navy.mil or call 866-793-4447.

Q: I need my notification letter sent to a different address. What can I do?
If you need the notification letter mailed to a different address, please email: N1Privacy.fct@navy.mil or call 866-793-4447 so we can accurately process your information.

Q: What if I have not received notification and think I'm affected?
If you believe you have been impacted by the PII security breach, Sailors may email: N1Privacy.fct@navy.mil or call 866-793-4447.

Q: What can I do right now to protect myself?
At this stage, there is no information to suggest misuse of the information that was compromised.

Here are steps you can take to help protect your identity:

- Check and monitor your (free) credit report for suspicious activity: https://ftc.gov
- Spot the warning signs of identity theft (IdentityTheft.gov has some examples)
- Be aware of phishing scams (both online and via phone)
- Update your passwords and use separate passwords for each account
- Monitor your financial accounts for suspicious activity
- Keep all security software up to date, use a firewall and email filter
- Get up to speed on computer security
- We recommend Sailors sign up for credit monitoring services if not previously enrolled

We encourage individuals visit the Federal Trade Commission's website (https://ftc.gov) for information on how to protect yourself from identity theft and what to do if you are a victim of identity theft.

For additional guidance on safeguarding your PII, we also recommend you visit the Federal Trade Commission's web site at: https://www.identitytheft.gov.