Defense Travel Management Office Vendor Data Breach Q&A
Updated November 13, 2018

Q1. When did the breach occur?
A1. Investigations are still being conducted, however, at this time preliminary findings indicate the initial infection and potential breach occurred as early as December 2017.

Q2. Was the affected system a DoD system?
A2. No, the system is owned by a commercial vendor under contract with the Department to provide travel services support, including the booking and ticketing of travel reservations. There is currently no evidence that the breach impacted any DoD systems, or that the use of Defense Travel System (DTS) alone is the basis for risk.

Q3. Has the vulnerability been fixed?
A3. The vendor is still under contract with DoD, however, the Department issued stop work orders so the vendor is not presently supporting the DoD’s travel mission while vulnerabilities are confirmed and remediated.

Q4. Were all DoD employees affected?
A4. No, at this time the Department estimates only a very small percentage of the total population of employees, approximately 27,600 travelers, were potentially affected.

Q5. Have the affected individuals been notified?
A5. The Defense Travel Management Office sent electronic messages to all potentially affected travelers on October 15, 2018. Follow-up notifications will be made shortly via U.S. Postal Service.

Q6. I did not receive an email notification; how do I confirm whether or not I was affected?
A6. Follow-up notifications will shortly be made via U.S. Postal Service. The notification will provide additional information on how to confirm if you were affected and how to initiate your identity theft services. If you have any questions, please contact ID Experts at (877) 900-5601.

Q7. What elements of my personal information were potentially breached?
A7. Traveler information maintained by the vendor includes Defense Travel System (DTS) profile information (rank/grade, home address, home telephone number, unit, work address, work phone number, travel purpose); emergency contact information (related to spouse or another applicable individual); Government travel charge card information (and in very rare instances, personal credit card information provided by the traveler); email address; DoD ID number; and TSA Secure Flight Passenger Data. Social security numbers are not included in this data.

Q8. I used my personal credit card for travel; what do I need to do?
A8. If you booked a lodging reservation in DTS that was not centrally funded, and in doing so entered your personal credit card information when prompted (Note - this is a very rare occurrence, especially for holders of a Government travel card), you should contact your credit card company to ensure against unauthorized use. Using your personal credit card only for meals and other incidental expenses would not create risk to the traveler concerning this potential breach.
Q9. What mitigation or protections are being offered to those whose information was stolen?
A9. Potentially affected Government travel credit cards are being canceled and replaced, and a separate/additional email has been provided to these cardholders. Identity theft protection services will also be offered for two years, at no cost, to all individuals whose information was potentially compromised. Travelers will receive additional details from the identity theft protection provider on activating this service shortly.

Q10. How do I get a new travel card if I am on TDY?
Q10. To avoid inconveniencing travelers while on TDY, cards will not be replaced until those travelers return from TDY.

Q11. I'm traveling in the next couple of weeks, do I need a new card before I travel?
Q11. A phased approached to travel card cancellation and replacement is underway, with those scheduled to depart getting replacement cards first. Should you find that you are scheduled to depart and have not yet received your replacement travel card, please contact your organization’s travel card Agency Program Coordinator for assistance.

Q12. What else can I do to protect myself?
A12. To minimize or mitigate potential identity theft, you may wish to review the actions outlined on the Federal Trade Commission’s Web site at: http://www.ftc.gov/bcp/edu/microsites/idtheft/. You may also wish to place a fraud alert on your credit. A fraud alert can be placed by contacting any of the three national credit reporting agencies, Experian, Equifax, and Transunion.