



**DEFENSE TRAVEL
MANAGEMENT OFFICE**

Chip and PIN Government Travel Charge Card Fact Sheet

I. Overview

On October 17, 2014, President Obama issued an Executive Order requiring federal agencies to upgrade payment cards and systems to employ enhanced security features, to include Chip and PIN technology. Effective January 2015, all Department of Defense Government Travel Charge Card (GTCC) holders will begin migrating to Chip and PIN cards.

Chip and PIN cards contain a microprocessor that requires cardholder authentication via a 4-digit Personal Identification Number (PIN) input at point-of-sale. The microprocessor chip encrypts the transaction data protecting the cardholders' personally identifiable information (PII), as well as the Government's sensitive transaction and payment data. If the card is lost or stolen, the embedded microchip makes the card extremely difficult to counterfeit.

II. Timeline

- Starting in January 2015, only Chip and PIN travel charge cards will be issued to DoD personnel to include qualified new applicants and individuals reporting their card lost/stolen.
- **Cards that expire between February and December 2015:** a Chip and PIN card will be issued approximately 30 days before the current cards expire.
- **Active accounts with cards that expire after 2015:** Accounts used at least once within the last 18 months, will be issued a Chip and PIN card sometime between July and October 2015.
- **Inactive accounts with cards that expire after 2015:** Accounts not used at least once within the last 18 months will be issued a Chip and PIN card approximately 30 days before the current card expires.

**The reissuance of Chip and PIN cards does not apply to centrally billed accounts (CBA).*

III. Additional Information

- To ensure maximum support of the DoD mission, new Chip and PIN cards will include both the magnetic stripe technology and the new Chip technology.
- Chip and PIN cards are issued on the quasi-generic grey plastic and contain a chip.
- Expiration dates and three digit security codes will change but account numbers will remain the same as long as the card is not being replaced because it was lost, stolen or compromised.
- **Before the new cards arrive,** cardholders should login to CitiManager (<http://www.citimanager.com/login>), Citi's online account management system, to ensure their contact information is up-to-date. Cardholders can also call the number on the back of the card to update their contact information.

- **When the card arrives**, cardholders must update their DTS profile with the new card information to avoid declines when making travel arrangements. For instructions, go to: http://www.defensetravel.dod.mil/Docs/GTCC_Profile_Update.pdf.
- **Instructions for first use:** Until cardholders complete their first Chip transaction at a staffed, chip-enabled point-of-sale, the newly selected PIN will not be recognized at subsequent chip-enabled self-service terminals (i.e., ATM). Instead, the Chip-enabled terminal will use the magnetic stripe instead of the Chip.

Working Together: Agency Program Coordinators and Defense Travel Administrators

IMPORTANT: Unless the card is reported as lost or stolen, the account number on the new Chip and PIN card will stay the same but the expiration date and three digit security code on the back of the card will change. It is important for Agency Program Coordinators (APC) and Defense Travel Administrators (DTA) to work together to ensure that Defense Travel System profiles are updated with new card information.

While you may be aware that many GTCC declines are a result of expired cards in DTS profiles, you may not know that this often results in higher Commercial Travel Office (CTO) transaction fees. A CTO cannot issue a ticket if/when DTS provides outdated GTCC information. When this happens, ticket issuance is delayed until the CTO can obtain a valid GTCC, which results in a higher CTO transaction fee, negatively impacting the organization's travel budget.

To combat this issue, DTAs and GTCC APCs should collaborate to ensure GTCC information in DTS is accurate and current for all applicable travelers. For example, a DTA can run the "Account Info List" report under "View Person Lists" in the People Module of the DTS DTA Maintenance Tool, and share it with their organization's APC. This report displays employee's name, last four of employee's social security number, and the GTCC account number and expiration date for each of the organization's employees with a DTS profile. The APC and DTA can quickly identify DTS profiles with an expired GTCC number. The APC can then obtain from Citi's Client Reporting System (CCRS) – Account Listing report, the current expiration dates for those expired cards previously identified in DTS. The organization's APC and DTA can jointly determine the most expedient means for updating the GTCC expiration dates or any other discrepancies in the DTS profiles.

IV. Resources

- [Frequently Asked Questions for APCs and DTAs](#)
- [Frequently Asked Questions for Cardholders](#)
- [How to Update Your DTS Profile](#)
- [How to Update DTS Authorizations with New Payment Information](#)
- [CitiManager](#)
- [Chip and PIN webpage on the Defense Travel Management Office website](#)