



**DEFENSE TRAVEL
MANAGEMENT OFFICE**

Chip and PIN Government Travel Charge Card Fact Sheet

I. Overview

In October 2014, President Obama issued an Executive Order requiring federal agencies to upgrade payment cards and systems to employ enhanced security features that included Chip and PIN technology. From January through October 2015, all Department of Defense Government Travel Charge Card (GTCC) holders with active accounts were converted to the new Chip and PIN technology. .

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

- Since January 2015, only Chip and PIN travel charge cards have been issued to DoD personnel. By the end of October of 2015 all accounts that were used at least once within the last 36 months have been issued a Chip and PIN card.
- **All remaining accounts are considered inactive and have** been placed in a soft close status for a period of six months. Accounts are considered inactive when the:
 - Cardholder failed to receipt verify the magnetic stripe card
 - Magnetic stripe card was receipt verified, but no merchant or ATM transactions were made within the last 36 months
 - Account credit limit is set to \$0
 - Account is flagged for an incorrect mailing address/returned mail
 - Account is flagged because of suspected fraud

Cardholders expecting to travel can contact Citi within the 6 month period to request a Chip and PIN issuance. All accounts that remain in a soft close status after six months will be permanently closed and cardholders will need to reapply to be issued a card.

** For centrally billed accounts (CBAs), the reissuance of Chip and PIN cards only applies to unit card accounts. Transportation-only CBAs will not be reissued as Chip and PIN.*

III. Additional Information

- Chip and PIN cards still include the magnetic stripe for those merchants that have not converted to Chip and PIN technology.
- Expiration dates and three digit security codes change, but account numbers remain the same as long as the card is not being replaced because it was lost, stolen or compromised.

- 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.
- If a cardholder you believes their account is inactive and he/she plans to travel within the next six months, they should contact Citi today to receive a Chip and PIN card replacement.

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.

Many GTCC declines are a result of expired cards in DTS profiles, often resulting 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](#)