

# Quick Reference Guide to Government Travel Charge Card Declined Authorization Codes

February 2026 – Version 1.0

*This table defines all declined authorization codes produced by DoW Government Travel Charge Card (GTCC) transactions in the last fiscal year. This data dictionary is updated annually. All definitions have been created in coordination with Citibank.*

CODE#	NAME	DEFINITION
2	Closed Account	The GTCC account has been officially closed, either by the cardholder or the issuing bank.
7	Card Expired	The expiration date on the card has passed, rendering it invalid.
8	Charge-off Account	The account has been closed and written off as bad debt due to prolonged non-payment. No transactions are permitted.
14	Credit Revoked	All credit privileges for this account have been permanently revoked by the issuing bank.
48	Not Enough Available Money	The transaction amount exceeds the available credit limit on the GTCC account.
49	Excess Decline Authorizations Today	The card has been declined too many times within a short period, triggering a velocity limit to prevent further attempts.
103	Invalid Card or Account	The card number or account information entered is incorrect or invalid.
111	Bad PIN	The Personal Identification Number (PIN) entered is incorrect. This usually applies to ATM withdrawals or debit-like transactions.
112	Exceeds ATM Daily Limit	The transaction would cause the total dollar amount withdrawn from ATMs in a 24-hour period to exceed the established limit.
113	Exceeds Number ATM Per Day	The cardholder has already made the maximum number of ATM withdrawals allowed in a 24-hour period.

CODE#	NAME	DEFINITION
114	Exceeds Bad PIN Limit	The cardholder has entered the wrong PIN too many times, and the card is now blocked to prevent unauthorized access.
124	Invalid CVV2 or CVC2	The card verification value (CVV2 is for Visa, CVC2 is for Mastercard) entered at the time of the transaction doesn't match the code on the back of the card. This is a security measure to prevent fraud.
125	Invalid Card Verification VAL/CHK	The card verification value (CVV2, CVC2) provided does not match the value on file for the card.
134	Card Activation	The card requires activation before it can be used. This is a security measure to ensure the card is in the hands of the legitimate cardholder.
146	Invalid CVC3/DCVV Value	A contactless/mobile payment security failure. The dynamic security code generated for the transaction was invalid.
147	Wrong Entry Mode for Card	The card was entered in a manner not permitted (e.g., the magnetic stripe was swiped on a chip-enabled terminal that requires the card to be inserted).
149	ATC Value Outside Window	An EMV chip security feature. The Application Transaction Counter (ATC) from the chip is out of sync with the bank's records, suggesting possible card cloning.
151	Duplicate ATC	An EMV chip security feature. The transaction was submitted with an Application Transaction Counter (ATC) that has already been used.
152	Exceeds Maximum RFID Amount	The transaction amount is over the limit allowed for a single contactless ("tap-to-pay") transaction.
162	Point of Sale Error	The decline originated from an error at the merchant's point-of-sale terminal, not from the issuing bank.
207	Invalid Expiration Date	The expiration date entered at the time of the transaction is not the same as the expiration date on the card.

CODE#	NAME	DEFINITION
453	Cannot Authorize During Downtime	The bank's authorization system was temporarily offline or unavailable to process the transaction request.
500	Coded Security Fraud - Lost	The card has been officially reported as lost by the legitimate cardholder.
501	Coded Security Fraud - Stolen	The card has been reported as stolen, and any attempted transaction is automatically declined. When a card is reported as stolen by the cardholder or APC a new card will be issued by the bank.
502	Coded Security Fraud - Not Received	The card was reported as mailed but never received by the cardholder, suggesting potential mail interception.
503	Coded Security Fraud - Fraud Application	The account was determined to have been opened using fraudulent or synthetic identity information.
512	Coded Security Fraud - 4F	The transaction was declined based on a specific internal fraud strategy or rule, identified by the internal "4F" code.
518	Coded Security Fraud - Account Takeover	The account is flagged due to a high suspicion that it has been compromised and is being used by an unauthorized third party.
519	Coded Security Fraud - Mail Or Phone	The transaction has been flagged as potentially fraudulent because it was initiated via mail or phone, which are considered higher-risk channels.
557	Watch	This flag indicates that the account requires further review or investigation by the card issuer due to potential fraud.
601	Exception File	The account is listed on an internal file (e.g., a watchlist) that flags it for automatic declines.
624	Active Service Member Plan	The account is associated with a service member covered by a protection plan (e.g., SCRA), which may have specific restrictions.

CODE#	NAME	DEFINITION
683	Decline for Past Due	The GTCC account has an outstanding balance that is overdue, and the card is being blocked until the balance is paid.
687	Account Closed/Blocked	The account has been permanently closed or is temporarily blocked from all transaction activity.
802	Card Not Effective	Card account is open but does not have a current active start and end date.
814	Account Number Limit Is Exceeded	The transaction exceeds the total number of transactions allowed for the account within a defined period (e.g., per day, per week).
818	Individual MCCG Amount Limit Is Exceeded	The transaction exceeds the spending limit set for a specific Merchant Category Code Group (e.g., a daily limit on travel or electronics).
823	Individual MCCG Include (No Match)	MCCG stands for Merchant Category Code Group. This means the type of merchant (e.g., restaurant, hotel, gas station) where the card is being used is restricted or not allowed due to DoD policy. The transaction is declined because the merchant's code doesn't match the allowed codes for that cardholder.
831	Invalid Request: Swiped But No Plastics	A swipe transaction was attempted on an account that does not have a physical card associated with it (e.g., a virtual-only account).
850	Bank Request: Fraud Strategy 1	A specific, proprietary fraud rule implemented by the bank was triggered by the transaction's characteristics.
870	Declined By Score 1	The transaction was declined because it triggered an internal fraud detection model. The risk score assigned to the transaction exceeded a predefined threshold.
881	ARQC Invalid	An EMV chip security failure. The Authorization Request Cryptogram (ARQC) sent from the chip could not be validated by the bank, indicating a potential data error or fraud.
882	Application Transaction Counter Invalid	An EMV chip security failure related to the transaction counter, indicating a data mismatch or potential fraud.

CODE#	NAME	DEFINITION
884	Transaction Not Allowed For Card	The type of transaction is not permitted for this specific card product (e.g., attempting a cash advance on a card that doesn't allow it).
901	Tiered Watch Level 1	The transaction triggered a low-to-mid-tier rule in an automated fraud monitoring system, placing the account on a watch list.