Visa Response Codes

Requirements and Best Practices

Version 1.0

9 March 2023

Important Information on Confidentiality and Copyright

Notice: This information is proprietary and CONFIDENTIAL to Visa. It is distributed to Visa participants for use exclusively in managing their Visa programs. It must not be duplicated, published, distributed or disclosed, in whole or in part, to merchants, cardholders or any other person without prior written permission from Visa.

The Visa Confidential label signifies that the information in this document is confidential and proprietary to Visa and is intended for use only by Visa Clients subject to the confidentiality restrictions in the *Visa Core Rules and Visa Product and Service Rules*, non-Client Third-Party Processors that have an executed and valid VisaNet Letter of Agreement on file with Visa, and other third parties that have a current participation agreement, including confidentiality provisions, or other non-disclosure agreement with Visa that covers disclosure and use of the information contained herein.

This document is protected by copyright restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Visa.

The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other trademarks not attributed to Visa are the property of their respective owners.

Note: This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

THIS PUBLICATION IS PROVIDED ON AN "AS IS, WHERE IS" BASIS, "WITH ALL FAULTS" KNOWN AND UNKNOWN. THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN: THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. VISA MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME. WHERE POTENTIAL FUTURE FUNCTIONALITY IS HIGHLIGHTED, VISA DOES NOT PROVIDE ANY WARRANTY ON WHETHER SUCH FUNCTIONALITY WILL BE AVAILABLE OR IF IT WILL BE DELIVERED IN ANY PARTICULAR MANNER OR MARKET. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VISA EXPLICITLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE INFORMATION CONTAINED HEREIN, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

If you have technical questions or questions regarding a Visa service or questions about this document, please contact your Visa representative.

Contents

Tables

Figures

Introduction

Visa drives improvements to encourage good business practices that can help issuers, acquirers, and merchants to reduce fraud, improve authorization approval rates, reduce operational costs, and enhance satisfaction. Ensuring appropriate information flow is critical to creating optimal behavior for all players within the ecosystem.

Authorization response codes can improve transaction processing by increasing transparency when an authorization is declined. Visa rules enable merchants to resubmit select declined transactions, so better use of appropriate codes can help to reduce unnecessary overhead of transaction reattempts.

This document provides the authorization response code requirements issuers must follow as well as best practices to clarify which authorization response codes are best suited to particular transaction scenarios. It is intended to help issuers more effectively use descriptive response codes to increase authorization approval rates by identifying the conditions that caused a decline, allowing a merchant to correct the issue and determine whether a subsequent reattempt is appropriate. Following both the requirements and best practices should improve financial performance for issuers and drive card use, engagement, satisfaction, and retention for cardholders. The guidelines are designed to:

- Increase transparency in declines
- Reduce unnecessary reattempts
- Allow acquirers and merchants to correct issues and optimize resubmission
- Allow issuers to identify the decline reason
- Help issuers achieve minimum approval rates by reducing excessive authorization reattempts
- Improve the payments ecosystem by optimizing behavior for all parties

Audience and Scope

This document is intended for issuers, to provide both their obligations and best practices for providing appropriate, descriptive response codes when declining an authorization request. It also gives merchants and acquirers descriptive information about decline codes to avoid indiscriminate authorization reattempt strategies or changes to data elements that can negatively impact approval rates.

Related Publications

Further details about authorization processing information are available in in the *V.I.P System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1*.

Note: This document replaces previous communications regarding response code best practices.

1 Overview

Cardholders anticipate usage of their Visa card will result in a successful purchase. However, declines are an important part of Visa card processing. Declines are meant to protect both the cardholder and the merchant from loss. Transaction declines can have negative consequences for cardholders, issuers, acquirers, merchants, and Visa, such as:

- Cardholder confusion, embarrassment, or inconvenience when they are unable to purchase goods or services
- Issuer losses when cardholder cannot complete the transaction or uses an alternate form of payment
- Merchant friction at the POS, customer service issues, or lost sales when the cardholder has no alternate payment method

As the channels and use cases enabled by card payments have increased, so have the overall percentage of declines, particularly in electronic and remote commerce environments. There are multiple causes for the increase in declines:

- Inconsistency in the information presented in the authorization request makes it difficult for the issuer to interpret the specific nature of the payment request
- Increases in subscription and recurring services, "free to fee" models in which payment occurs after the service is provided
- Machine-learning capabilities that manipulate transaction data for either legitimate or nefarious purposes

Card acceptance is dependent on improving transaction results that grow and protect all stakeholders. Improving the cardholder and merchant experiences benefits all participants in the payments value chain. Issuers should strive to reach or exceed required authorization approval rates, as they manage risk to provide a positive consumer experience. Following the requirements and best practices set out in this document will help increase approvals of legitimately re-attempted transactions.

Using accurate response codes allows an issuer to better understand its portfolio and continue to refine its authorization strategies. Issuers can collect, aggregate, and analyze the response codes of declined transactions. Through this practice, issuers can gain vital insights into their transaction patterns and develop remedial strategies and actionable solutions.

Sending accurate and descriptive decline response codes allows merchants and acquirers to take appropriate action to fix an issue that caused a decline. Furthermore, when an issuer's decline indicates that the issuer will never approve the transaction, the merchant must not retry the request, thereby saving all stakeholders unnecessary processing and operational costs.

The potential consequences of inaccurate response codes from issuers are that merchants and acquirers may develop authorization reattempt strategies that:

- Are overly aggressive and can look like fraud or denial of service attacks against an issuer host
- Result in changing data elements, which damages analytics and detection model performance
- Require unnecessary authorization bandwidth, creating greater costs for all participants
- Negatively impact issuer approval rates when the same transaction is declined multiple times

Issuers that fail to follow these requirements will mislead merchants, resulting in excessive retries or preventing legitimate transactions from being approved. Acquirers and merchants may not have confidence that a decline is the result of a temporary condition, such as lack of funds, or a more severe condition, such as an invalid card number or fraud condition.

2 Response Code Categories

Response codes communicate the issuer's decision about a request. Requests can involve monetary and nonmonetary events. The issuer's approval or decline of an authorization request is communicated in the Authorization Response Code located in Field 39 of the Visa message specification.

The following Authorization Response Codes indicate issuer approval of a request:

- 00 = Accepted or Approved
- 10 = Partial Approval
- 85 = No Reason to Decline (for select transactions)

All other response codes indicate an issuer decline response. Visa rules categorize decline response codes into four categories to help acquirers and merchants understand whether request reattempts are possible. The categories are:

- Category 1: Issuer will never approve (Reattempt not allowed)
- Category 2: Issuer cannot approve at this time (Reattempt allowed)
- Category 3: Data quality (Revalidate data prior to reattempt)
- Category 4: Generic response codes (Reattempt allowed)

The following sections describe the categories and best practices for each case. Detailed definitions of each response code and its corresponding category are described in Table A–1, Response Code Details and Issuer Recommendations in Appendix A.

2.1 Category 1: Issuer Will Never Approve (Reattempt not Allowed)

Category 1 response codes must only be used to indicate a permanent condition that cannot be fixed by the merchant. For example, a Category 1 response can be used to indicate:

- The account never existed or has been permanently blocked, including lost or stolen account numbers
- The account is invalid
- The transaction is not permitted due to permanent product or regulatory restrictions
- Transaction error conditions exist that prevent approval (a Visa system used by the issuer has determined that the transaction cannot be accepted)

Requirements and Best Practices for Category 1 Codes

- Issuers must not use the response codes in this category for temporary decline conditions. For temporary account restrictions, issuers must use response codes from Category 2.

- Issuer must only use Category 1 response codes for account numbers or transactions that will never be approved.
- Use of this category prevents the transaction from being completed, so it is imperative that the issuer only use Category 1 responses when absolutely necessary.
- Visa will monitor issuers for minimum approval rates and will evaluate the percent of declines issued from Category 1. Compliance action may be taken in case of inappropriate usage of Category 1.
- In-store cardholder-initiated transactions that are declined in this category may result in a request for an alternate form of payment or in a lost sale.
- An acquirer or merchant must not permit a reattempt request that was previously declined in this category and must have controls in place to avoid reattempts. Such a reattempt will cause an additional System Integrity Fee to be assessed.
- Acquirers and merchants should implement use of Visa Account Updater to avoid a reattempt after receiving a response code that indicates a Closed Account and contact the cardholder for the updated payment credential

2.2 Category 2: Issuer Cannot Approve at this Time (Reattempt Allowed)

Category 2 response codes indicate the issuer may approve the request in the future but cannot do so at the time of the request. This could be due to a temporary decline condition such as credit risk, issuer velocity controls, lack of available funds, or other account restrictions. The response indicates that the issuer would welcome a future authorization attempt. In some cases, cardholder or merchant action may be required to remove the restriction before an approval can be obtained.

Requirements and Best Practices for Category 2 Codes

- Issuers must never use the response codes in this category for permanent account decline conditions.
- Issuer should ensure that all authentication actions have been verified prior to issuing a decline from this category.
- If a prepaid account is perpetually in an insufficient funds status after 30 days, the issuer may consider issuing an account closed response. This is also true for debit accounts that remain in an insufficient funds status for an extended period (for example, longer than 3 months).
- An acquirer or merchant is permitted to reattempt authorization up to 15 times over 30 days.
- Any suspected fraud response on a cardholder-initiated transaction should immediately refer the cardholder to the issuer for resolution. When the issuer provides the cardholder with confirmation that the sale will be accepted, only then may a reattempt be processed.

- Acquirers should monitor suspected fraud responses from all merchant-initiated transactions and prevent all reattempts from the same merchant, since the cardholder cannot perform any action to rectify.
- Merchants should monitor suspected fraud responses and implement:
  - Controls to ensure legitimate purchase data has been provided
  - Velocity controls to prevent enumeration or brute force attacks

2.3 Category 3: Data Quality (Revalidate Data Prior to Reattempt)

Category 3 codes are used to indicate data quality issues in which invalid payment or authentication data has been provided and that the issuer will approve the transaction if valid information is provided. High occurrences of response codes in these categories may indicate insufficient merchant risk protection controls such as velocity checks or pre-validation of basic account information (e.g., mod-10 or expiry date).

Requirements and Best Practices for Category 3 Codes

- Declines in this category should be monitored for fraud and velocity parameters. Category 3 declines usually arise from card or account testing that results in authentication or verification failure.
- Issuer may use fraud monitoring services or artificial intelligence to score and detect complex failure patterns that could be the result of enumeration events.
- An acquirer or merchant is permitted to reattempt authorization up to 15 times over 30 days. Nevertheless, it is recommended that acquirers and merchants do not reattempt a request with a Category 3 decline more than three times.
- After no more than three attempts at the same merchant, marketplace, or wallet originating from the same or different acquirer, the issuer should return a response code from Category 1 for those transactions.
- Merchants should implement:
  - Controls to ensure legitimate purchase data has been provided
  - Display messaging on the POS terminal or payment page to prompt the cardholder to correct invalid payment information
  - Using Visa Account Updater to obtain updated payment credentials when receiving a response code that indicates an expiration date error
  - Velocity controls to prevent enumeration or brute force attacks

2.4 Category 4: Generic Response Codes (Reattempt Allowed)

All remaining decline response codes not specified in categories 1–3 are considered generic response codes. Generic response codes do not provide the acquirer or merchant with meaningful information for effectively managing a reattempt strategy.

Requirements and Best Practices for Category 4 Codes

- Generic response codes (such as "Do Not Honor") must only be used infrequently and on an ad-hoc basis when there is no specific decline code to describe the reason for the decline.
- Services that permit the cardholder to block transactions from select merchants or channels should use response codes from Category 4. Only services that allow the cardholder to change the parameters of the block should lead to a Category 4 response. For the small number of instances where the block cannot be changed, a Category 1 code must be used.
- Acquirers and merchants are permitted to reattempt any request that receives a Category 4 decline.

2.5 Summary of Decline Code Categories

Table 2–1: Summary of Decline Code Categories

Category	Required Behavior and Best Practice	Applicable System Integrity Fee
1	Do not reattempt Issuers must limit use of Category 1 declines to credentials that will never be approved (such as compromised accounts) or to transaction types that are permanently restricted and will never be approved	Never Approve Reattempt Fee is assessed to the acquirer for each reattempt of a declined transaction when an issuer responds with a Category 1 response code
2	Limit reattempts to 15 in 30 days	Excess Reattempt Fee is assessed to the acquirer for each transaction reattempt in excess of 15 within 30 days
3	Revalidate data prior to reattempt, monitor for fraud attacks	Data Quality Fee is assessed to the acquirer if the merchant request count resulting in Category 3 response codes exceeds the regional tolerance threshold
4	Minimal use of generic response codes	Generic Response Code Excess Use Fee is assessed to the issuer for each transaction declined with a Category 4 code in excess of the maximum threshold allowed

3 Authorization Requests

Many different types of transaction are sent through the authorization system. Understanding the nature of a request is a key to effectively managing the response. Authorization requests can be categorized as non-monetary or monetary transactions.

- Non-monetary requests are used to gather and verify information. Typically, these occur prior to the initiation of a monetary authorization message.
- Monetary transactions seek approval for a specific account and a defined monetary amount. When approved, these requests result in a movement of funds between the participants, commonly known as payment.

Non-monetary requests often occur in advance of a monetary transaction and their responses can form the basis of the decisions that will also apply to monetary transactions.

3.1 Non-Monetary Requests

Account verification messages are the most common non-monetary requests. These messages allow the assessment of a credential prior to a monetary transaction. The following methods of account verification[1] are used:

- Key-entered—the most common type of account verification. The cardholder or merchant key-enters the PAN, expiration date, and optionally a CVV2.
- Stored credentials—used when merchants or token requestors store payment credentials to simplify the user experience when shopping. The application provider or merchant attempts to determine if the PAN on file is still valid. These requests contain the PAN and the expiration date.
- Terminal-generated requests—used when the merchant is seeking the highest level of assurance that the PAN is valid. These requests contain magnetic stripe or chip cryptograms and cardholder verification data.

Account verification messages are used to support all non-monetary requests and are identified by the presence of value **51** in V.I.P. Field 25 – POS Condition Code, along with a zero-dollar amount in V.I.P. Field 4 – Amount, Transaction, in the authorization request.

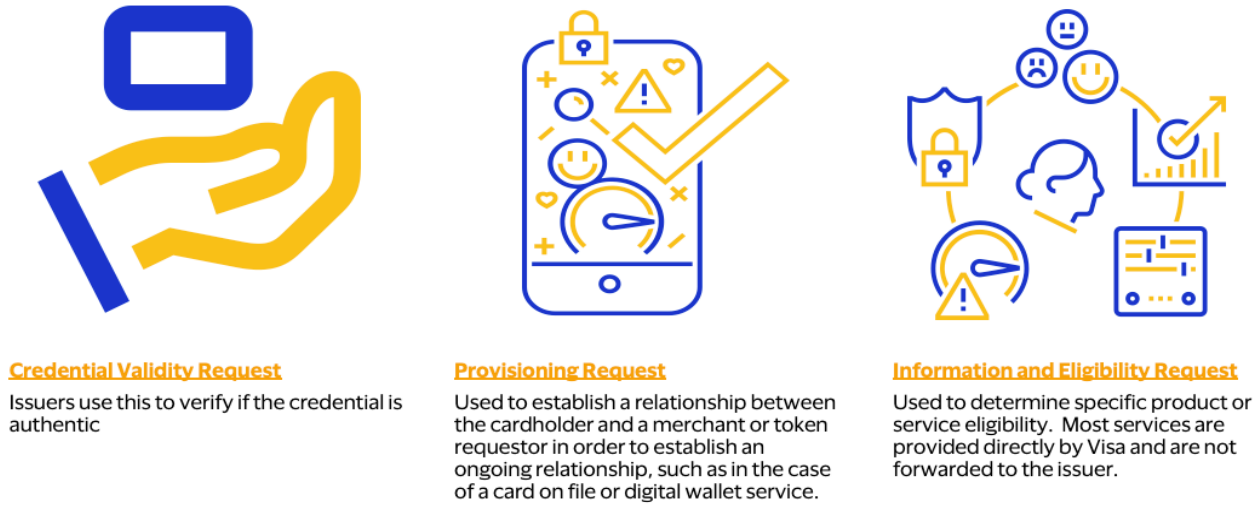
Account verification requests fall into three categories (Figure 3–1):

- Credential validity requests (account verification)
- Stored credential provisioning requests

[1] An issuer may determine the method by evaluating the value in V.I.P Field 22 – POS Entry Mode

- Information and eligibility requests

Figure 3–1: Account Verification Request Categories



The following sections describe these types of requests.

3.1.1 Credential Validity Requests

Credential validity requests are used by merchants to establish that a credential (PAN or token) presented at the point of transaction is currently active and valid. Issuers are requested to verify that the credential presented, and corresponding data is legitimate.

There are four types of credential validity requests that can be used to ascertain the authenticity of a Visa payment credential (Table 3–1). Each credential validity request is standalone and meant to be evaluated as a single event.

Table 3–1: Types of Credential Validity Requests

Type of Request	Purpose	Validation Recommendation
Basic Account Verification – No Verification Data	Establishes that the credential presented is legitimate and is assigned and active.	Validation is based on the PAN and the expiration date.
Account Verification – Static Data[2] (e.g., CVV, CVV2, AVS)	Establishes that the credential presented is legitimate and is assigned and active, and verification of possession is entered by the user.	Validation is based on the PAN, the expiration date, and the data collected from the user.

[2] The verification data collected is transmitted as clear text along with payment and expiration data. Static data is used to verify the legitimacy of the account and as a result can be phished from the consumer. Issuers should employ additional risk considerations before issuing an approved response.

Type of Request	Purpose	Validation Recommendation
Account Verification – Dynamic or Encrypted Data (Cryptogram, dCVV2, CAVV, PIN)	Establishes that the credential presented is legitimate and provides unique authentication data that can be verified by the issuer as a legitimately issued credential.	The data used to validate the payment credential is cryptographically protected and cannot be intercepted or modified using unsophisticated processes. Visa may provide an evaluation of the authenticity of the dynamic data presented.
Stored Credential – Account Verification	Establishes that a previously stored credential is still valid and in good standing.	This request mirrors a basic Account Verification – No Verification Data; however, the request should contain a value to indicate the purpose of the storage.

Field definitions are described in Table A–4, Field Level Details of a Message in Appendix A.

3.1.2 Stored Credential Provisioning Requests

A stored credential provisioning request is used to support the storage of a PAN or token in a merchant card-on-file solution or to facilitate token provisioning via the Visa Token Service for an eligible token requestor. These requests establish a consumer-consented relationship between the cardholder and a merchant or token requestor. The account verification request must include the basis for storing the credential (recurring, installment, or unspecified). An approval indicates that an ongoing relationship can be established, such as in the case of a card-on-file or digital wallet service.

Two types of stored credential provisioning requests are delivered through the authorization system:

- PAN Provisioning Request—establishes an ongoing relationship between a merchant and a cardholder
  - Should be considered a long-term permission for the merchant to retain access to the cardholder PAN without the cardholder having to present the payment credential (PAN and expiration date) for each subsequent transaction.
  - Must contain a value in the POS environment field that identifies the nature of the relationship the cardholder will have with the merchant (unscheduled, installment, or recurring).
  - One PAN can be stored with many different merchants and the issuer cannot deactivate the relationships unless a Visa Stop Payment Order is initiated.
- Token Provisioning Request—initiated using an account verification or token activation request message sent to the issuer by VTS to validate the PAN along with presented verification or authentication data
  - Establishes an ongoing relationship between the cardholder and the token requestor.

- Should be considered long-term permission for the token requestor to retain access to a unique credential that is valid in the token requestor's environment per token domain control restrictions.
- Issuers should evaluate the Acquirer ID (Field 32) and the VTS Service (Field 43) to identify an account verification or token activation request originated for token provisioning.
- Token for token provisioning requests establish an ongoing relationship between the cardholder and the merchant when a token is presented for storage.
  - Should be considered long-term permission for the merchant to retain access to a unique credential limited to the requestor's environment.
  - Allows a token requestor to request a new token using a valid and active source token.
  - Visa Token Service ensures that a low-value token cannot be used to create a high-value token without the issuer's ability to perform identification and verification (ID&V).

3.1.3 Information and Eligibility Requests

Account verification requests are used to determine specific product or service eligibility. Visa directly provides responses for most product and service eligibility requests and does not forward them to the issuer. For more details, refer Processing Code 39 in *V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1*.

Product eligibility and information requests originate from merchants, acquirers, and other third parties seeking information on a credential's eligibility to support specific transaction types or services. These requests are not forwarded to issuers, except under exception conditions where Visa does not have access to the information. The most common examples are Original Credit Transactions, cash disbursements, gambling, and deposits.

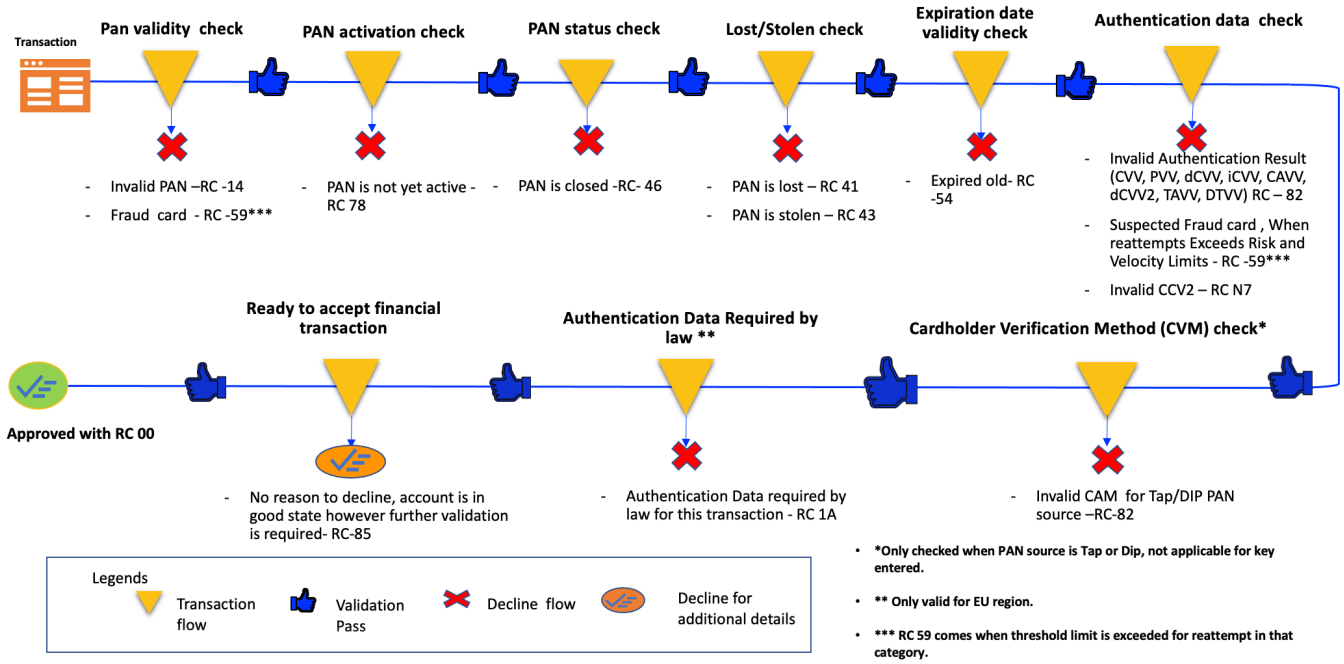
3.1.4 Issuer Requirements and Best Practices for Non-Monetary Response Codes

This section shows a common flow of a non-monetary transaction request. Figure 3–2 depicts sample steps and conditions that might be considered when evaluating a non-monetary request along with the recommended response codes.

Note: Issuers are free to evaluate these conditions in any order that is appropriate, and the figure is meant to represent common decisions considered during response code evaluation. Other conditions or questions are possible and may result in additional outcomes.

Details and recommendations for response codes can be found in Appendix A.

Figure 3–2: Sample Non-Monetary Request Flow



Successful issuer responses reflect the presentation method and data provided in the request, as shown in Table 3–2.

Table 3–2: Issuer Approval Codes by Account Verification Method

Type of Credential Validity Request	Method of Account Verification		
	Key-Entered	Stored Credential	Terminal
Basic Account Verification	85	85	N/A
Account Verification with Static Data	85	85	00
Account Verification with Dynamic Data	00	00	00

The evaluation of a non-monetary request includes an assessment of the conditions described in Table 3–3.

Table 3–3: Assessment of Non-Monetary Requests

Action	Assessment Condition	Failure Reasons
PAN Validity Check	Is the PAN on the issuer's cardholder master file?	Invalid Account (Never Issued)
Expiration Date Validity Check	Does the expiration date match one assigned by the issuer?	Invalid Expiration Date (Expired old/Never created)

Action	Assessment Condition	Failure Reasons
Authentication Data Check	Are verification or authentication data results successfully calculated?	Invalid Authentication Result (CVV/PVV/CVV2/CAVV/ Cryptogram)
PAN Activation Check	Has account activation occurred?	Inactive Account (Activated Required)
PAN Status Check and Eligible for Financial Transaction Check	Is the account open and able to accept transactions?	Invalid account status (Closed Account/Suspended)
Card Verification Method and Authentication as per Regulation Check	Is a Cardholder Verification Method (CVM) or Authentication Data required by law for this transaction (Europe only)?	Request Authentication Data (Cardholder authentication data required)
Exceeds Risk and Velocity Limits	Does the request contain a score that indicates it is high risk?	Suspicious Transaction (Suspected Fraud)

3.2 Monetary Transaction Requests

Monetary transactions are the most common authorization requests (Figure 3–3). A monetary transaction is used to request approval for a specific transaction and currency amount for a cardholder from a merchant or other provider. The primary objective is a determine funds availability and risk assessment. Monetary requests should be considered based on the event and risk level along with funds availability.

Figure 3–3: Monetary Transactions

Purchase of Goods and Services
- Card Present
- Transit, Grocery, Fuel

Purchase of Good and Services
- Card Not Present
- Subscription, Bill Payment

Visa Direct
- P2P, A2A, B2B, B2b

ATM
Cash Withdraw

There are five categories of transactions:

- Cardholder Initiated Transactions (CIT)—Authorization always involves the active participation of the cardholder and provides evidence that the cardholder presented the request. Evidence of cardholder presentment involves verification or authentication data in the request, and for some use cases, a Stored Credential indicator. A CIT may be a purchase of goods, services, or currency and can occur in both a card present and card not present environment.
- Merchant Initiated Transactions (MIT)—Authorizations do not involve the active participation of the cardholder but provide evidence that a previous cardholder interaction with the merchant exists. Merchant originated purchases do not have verification or authentication data but do contain other indicators that identify the reason or environment associated with the purchase. All MITs must contain a link to the original cardholder event via the Transaction Identifier.
- Cash Transactions—A cash transaction always involves the cardholder and some form of cardholder verification method based on either whether it originates from an attended or unattended environment. Cardholder Verification Methods (CVMs) can include a Personal Identification Number, a cardholder device authentication method (CDCVM), or device authentication results such as biometrics. Any transaction where cash is involved, whether it is cash withdrawal or cash back, should include a cardholder verification method.
- Refunds or Credits—A refund or return request will return funds to a cardholder for a previous purchase. Some refunds contain a link to the original event (Original Transaction ID), while others may not. In the case of credit/purchase returns, the recommendation is to use **85** instead of **00** (same as a deposit transaction), Funds should not be available until the transaction is completed.
- Undefined Purchases—An undefined purchase does not clearly indicate if it is cardholder originated or merchant originated. These transactions may be declined more often than CIT and MIT transactions since message data may not contain authentication or verification data that can be evaluated. Issuers may consider this type of transaction riskier than CIT or MIT transactions.

3.2.1 Authorization Decisions for Payment Credential Types

Payment credentials include Primary Account Numbers (PANs) and Visa tokens. The type of payment credential presented by the merchant will influence an issuer's authorization process.

- PANs are created by issuers and distributed to cardholders through an activation process they manage. Once issued and activated, the PAN can be used at many merchants using multiple payment technologies and in many different transaction environment and channels. Merchants may elect to store PAN data using the stored credential processing infrastructure to offer convenience for cardholders when shopping. A stored PAN is not unique to the merchant or wallet provider that elects to store it, making authorization processes more complex and subject to increase payment risk.
- Visa tokens are created through token provisioning. A token is a unique, 16-digit proxy value created and stored by the token requestor for use in transactions with the designated cardholder. They ensure that the cardholder has established a relationship with the token requestor for use within a defined and limited transaction environment. This model allows the

issuer to better understand and manage payment risk, along with the nature of the payment transaction presented. Unlike PANs, where verification data is optional in authorization requests, all Visa tokens processed on VisaNet will contain dynamic network verification data and authentication results that provide added payment risk management.

PAN transactions, especially in card-not-present environments, generally contain fewer data elements related to authentication and verification, making authorization decisions complex and more susceptible to fraudulent attacks. Tokens contain dynamic verification data, which is not re-usable, eliminating some of the authorization complexity and reducing some of the overall payment risk. Payment credential usage for different transaction categories is described in Table 3–4.

Table 3–4: Authorization Decisions for Payment Credential Types

Transaction Category	PAN Presented by Merchant	Visa Token Presented by Merchant
Cardholder Initiated Transaction	• Purchase environment determines if verification or authentication data is presented	• Always includes VTS verification data • Always contains the token requestor
Merchant Initiated Transaction	• May include original transaction reference • Includes MIT type	• Always contains the original transaction reference • Always includes MIT type • Always contains the token requestor
Cash Transaction	• Always has Card Verification Method such as PIN	• Always includes verification of CVM (e.g., CDCVM and device cryptogram)
Refund/Credit Return	• May contain verification or authentication data	• Always contains the token
Undefined Purchase[3]	• Always key-entered with no verification or authentication data present	• N/A; all token transactions are either CIT or MIT

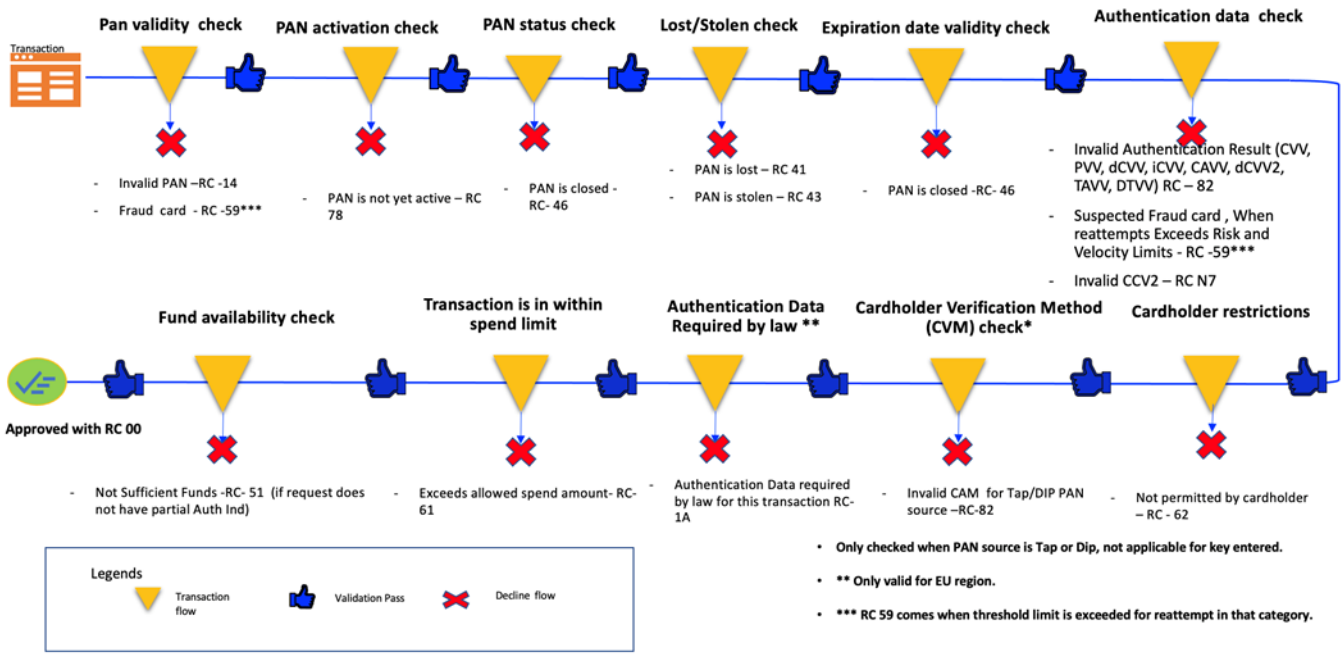
3.2.2 Issuer Requirements and Best Practices for Monetary Transaction Response Codes

Figure 3–4 depicts the steps and conditions to consider when evaluating a monetary transaction request along with recommended response codes. Issuers are free to evaluate these conditions in any order that is appropriate, and the figure is meant to represent common decisions considered during response code evaluation. Other conditions or questions are possible and may result in additional outcomes.

[3] Undefined purchases have the highest percentage of declines due to the lack of key transactions indicators necessary for increased approval rates.

Details and recommendations for response codes can be found in Appendix A.

Figure 3–4: Sample Monetary Transaction Request Flow



It is possible that multiple decline conditions could apply to a single transaction. The issuer must always select the most severe reason for decline. For fund-related declines (Not Sufficient Funds or Exceeds Daily Limit), the issuer must always evaluate funds availability as the last decision, as these response codes communicate that all other aspects of the transaction were evaluated and the only condition for decline is funds availability.

Successful issuer responses reflect the presentation method and data provided in the request (Table 3–5).

Table 3–5: Issuer Approval Codes by Transaction Category

Transaction Category	Approval Codes
Cardholder Initiated Transactions	**00, 10, 11**
Merchant Initiated Transactions	**00, 10, 11**
Cash Transactions	**00, 11**
Undefined Purchases	**00, 10, 11**
Refund/Credit Returns	**00** if reference (Tran ID) present **85** if reference (Tran ID) is not present

Note: Response code **85** is not allowed in monetary responses except for Refunds. When presented in a credit voucher, it represents an approval. For all other CIT, MIT, or undefined purchases, it must be treated as a decline.

The evaluation of a monetary transaction request is similar to a non-monetary request but includes added considerations for type of transaction, credit risk, and transaction amount. Table 3–6 describes the minimum authorization-based evaluations that should be considered. Visa provides additional fraud and risk tools that can assist issuers in their evaluations.

Table 3–6: Assessment of Monetary Transactions

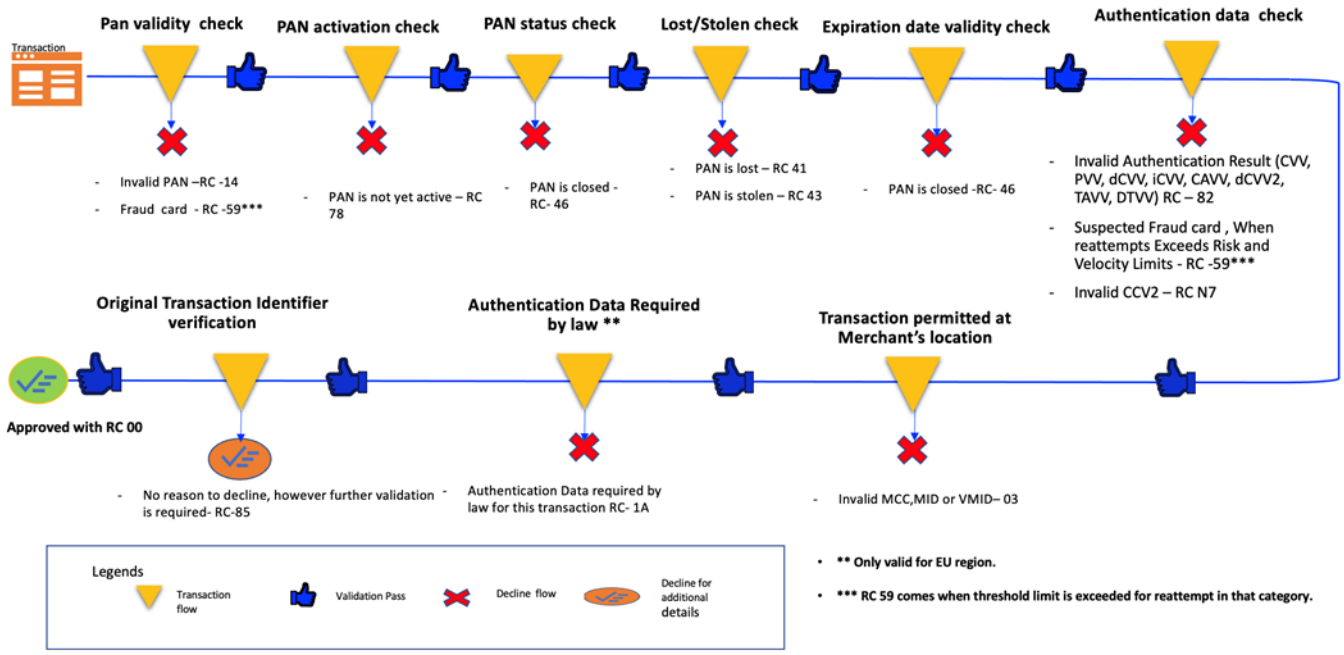
Action	Assessment Condition	Failure Reasons
PAN Validity Check	Is the PAN on the issuer's cardholder master file?	Invalid Account (Never Issued)
Expiration Data Validity Check	Does the expiration date match one assigned by the issuer?	Invalid Expiration Date (Expired old/Never created)
Authentication Data Check	Is verification or authentication data results successfully calculated and verified?	Invalid Authentication Result (CVV/PVV/CVV2/CAVV/ Cryptogram)
PAN Activation Check	Has account activation occurred?	Inactive Account (Activated Required)
PAN Status Check and Eligible for Financial Transaction Check	Is the account open and able to accept transactions?	Invalid account status (Closed Account/Suspended)
Authentication Limitation Per Regulation Check	Are there regulatory limitations on this transaction?	Disallowed Transaction
Fraud Check	Does the transaction pass fraud evaluation checks?	Suspected fraud
Cardholder Restrictions Check	Are cardholder restrictions associated with the transaction?	Not permitted by cardholder
Cardholder Verification Method Check	Is accepted Cardholder Verification Method (CVM) or Authentication Data required by law present in this transaction (Europe only)?	Request Authentication Data (Cardholder authentication data required)
Transaction Limit Check	Is the transaction within spend velocity?	Exceeds spending limit
Fund Availability Check	Are sufficient funds/spend available?	Insufficient funds

Action	Assessment Condition	Failure Reasons
Purchase Return or Credit Original Transaction Identifier and Amount Check	Does the transaction have an Original Transaction Identifier or original spend amount?	Need more details to verify the transaction

Note: Jurisdiction may influence the transaction approval decision. Issuers should consider the transactional jurisdiction when making an authorization or decline decision, as regulatory requirements may stipulate conditions that affect the outcome of the transaction. For Domestic Only card programs, evaluation of eligible jurisdiction may be required and, if not within country, decline using Category 1.

In the case of Refund or Credit Return transactions, issuers must perform basic authentication of the account as shown in Figure 3–5.

Figure 3–5: Purchase Refund or Credit Return Transaction Flow



3.3 Reattempting Declined Requests

Merchants can reattempt authorization requests that were declined due to Category 2, 3, and 4 codes. Reattempts are generally associated with card not present transactions, but in limited instances occur in POS environments. In general, face-to-face transactions are not reattempted by merchants unless some form of local or offline approval process has been performed, such as in the case of grocery, fuel, or transit purchases in which the initial transaction was identified by the merchant as a deferred authorization request.

In a face-to-face environment involving a chip or contactless transaction request, reattempts are not possible unless first presented as a deferred authorization request. A merchant should submit a deferred authorization request to allow the issuer to validate the required dynamic data and ensure the validity of the credential. This is necessary because contact and contactless chip transactions are protected by dynamic data and a transaction counter that is linked and uniquely tied to a specific transaction. The subsequent reattempt performed after the initial decline is presented as a card not present transaction using the Merchant Initiated Transaction (MIT) infrastructure.

A merchant that receives a Category 1 decline must never make subsequent authorization requests using the credential that received the decline.

After Category 2, 3 and 4 declines, a merchant may reattempt the declined authorization request up to 15 times in 30 days. "Reattempt " means resubmitting the authorization request for the same amount using the same credential. This means an authorization request for the same amount using a different credential is not considered a reattempt, nor is an authorization request for a different amount using the credential that received the original decline.

Acquirers and merchants are required to consistently use key data elements in merchant reattempts. Data manipulation will result in a compliance assessment.

Repeated reattempts above the threshold (up to a maximum of 15 over 30 days) or reattempt transactions that receive Category 1 response codes, or where the key data is manipulated to circumvent issuer authorization processes, will result in the assessment of fines to the acquirer.

3.3.1 Reattempt Evaluation Criteria

A transaction is considered a reattempt when the transaction originates from the same merchant and does not include dynamic data or verifiable data (excluding Address Verification Service (AVS) data).

If key merchant identifiers assigned by Visa are not included in the authorization request message, the system cannot accurately evaluate reattempt volume for a merchant. Visa expects merchants to send the fields in Table 3–7, which are used to evaluate if a transaction is a as reattempt. The absence of these key fields could result in consideration of reattempt of transaction.

If any of these field are not available to merchants, please contact VISA for details.

Table 3–7: Key Fields to Evaluate Reattempts

Field	Details
Field 2	Primary Account Number (PAN)
Field 3	Processing Code
Field 11	Only Considered in Terminal transaction
Field 12	Time of CIT, for MIT it should be fixed

Field	Details
Field 13	Date of CIT Interaction or Cardholder billing instruction
Field 43	Merchant Name or "url" for CNP merchants
Field 62.7	Must be a unique purchasing order; can be confirmation or receipt number
Field 62.20	Merchant Verification Value (MVV)
Field 63.3	Message reason code For MIT transactions if the merchant receives a decline due to insufficient funds and service has already been delivered to the cardholder. In such scenarios, merchants should resubmit transaction with reason code 3901 instead of reattempting the transaction.
Field 104	Dataset ID 56 - Payment Facilitator Data and sub merchant ID
Field 126.5	Visa Merchant Identifier (VMID)
Field 126.9	Cardholder Authentication Verification Value (CAVV)/TAVV
Field 126.10	Card Verification Value 2 (CVV2) in case of CNP

3.4 Use Cases

This section presents common use cases and real examples that can help in visualization of authorization request flows.

Figure 3–6: Ride Share (Approved Transaction)

Figure 3–7: Digital Currency Purchase (Visa Response with Information and Eligibility)

Rey opens an account on a digital currency platform in order to purchase digital currency, and adds their Visa credit card to the account

Provisioning

Their credit card is not eligible to purchase digital currency, so the credit card addition fails

Information and Eligibility

Rey then adds their Visa debit card to the digital wallet, and the card and credentials are authenticated

Credential Validity

They then purchase a small amount of digital currency

Financial Transaction

Figure 3–8: Subscription (CNP, Insufficient Funds, Invalid Expiration Date)

Evie opens an account with an internet music streaming service and adds her Visa credit card for recurring billing

Provisioning

The internet streaming service authorizes her account and card before charging the first month

Credential Validity

They continue to charge her card every month for a year

Financial Transaction

After one year, Evie receives a call from the music streaming service that her card was declined

Figure 3–9: Transit (CP, Prepaid with Insufficient Funds with Partial Auth?)

Q is starting a new job and plans to take public transit to commute to and from work

She plans to purchase a one-year transit pass to ride the local train

She attempts to use her Visa Prepaid Card to pay for the pass

Financial Transaction

Figure 3–10: Merchandise Return (CNP, Return, Credit Processing)

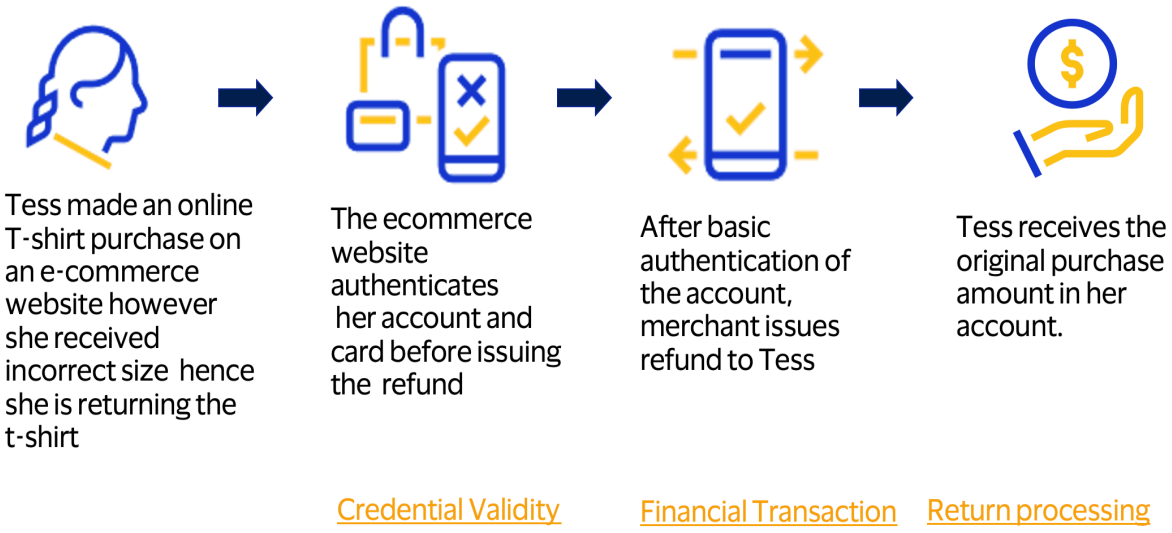


Figure 3–11: Overpayment to the Credit Account

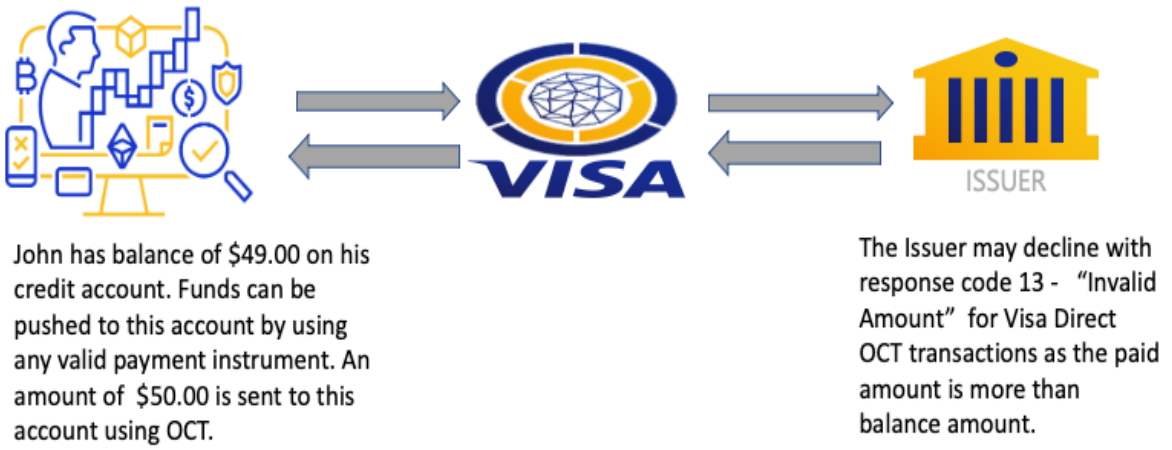


Figure 3–12: Temporarily Blocked Payment Credential

Tina

Robert

Tina and Robert have their profiles on e-commerce website. They use single payment credential for their purchases.
Robert has requested issuer to block transaction request for this credential.
Issuer has put temporarily hold on this credential due to Robert's request.

Tina made e-commerce purchase of a digital goods using same credential for which Robert has requested to block the transaction

The e-commerce website sends transaction details for authorization

VISA sends authorization request to Issuing Bank

ISSUER

The Issuer may decline with response code 78 - "Temporarily Blocked card".

Decline of Financial Transaction when payment credential is temporarily blocked

A Appendix

This Appendix includes the following tables:

- Table A–1: Response Code Details and Issuer Recommendations
- Table A–2: Response Code Details and Merchant/Acquirer Recommendations
- Table A–3: Response Code Definitions
- Table A–4: Field Level Details of a Message

Table A–1: Response Code Details and Issuer Recommendations

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
Approval	Not Applicable	**00**	Approval and completed successfully		An approval constitutes a confirmation that the PAN presented has been issued, is in an active status (is activated), account is in good standing, and sufficient data authentication has been performed. Issuer must not approve an Account Verification (AV) if they would not subsequently approve a "for value" authorization (Insufficient Funds notwithstanding); must not treat an AV as an authorization request (e.g., for single-use products, the AV doesn't count as the "single use").
		10	Partial approval		If a transaction contains a Partial Authorization Request indicator[4], then the issuer should approve with response code 10 for the available fund and should not decline with RC 51.
		11	Approved (V.I.P.)		
Accepted	Not Applicable	**85**	No reason to decline a request for address verification, CVV2 verification, or credit voucher or merchandise return		A "no reason to decline" is a confirmation that the payment credential presented has been issued and contains valid expiration date.
1	No reattempts allowed	**04**	Pick up card (no fraud)		Use for scenarios where the account has been closed, typically for non-fraud reasons.
		07	Pick up card, special condition (fraud account)		Use for accounts closed due to fraud or collections. Issuer must limit use to File Update messages (0302) from issuer to Visa.

[4] Partial authorization is required for all prepaid programs. It is optional but highly recommended for consumer debit and credit as well as commercial programs.

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
		12	Invalid transaction	Yes	Issuer should only use this response code when integrated Circuit Card (ICC) CVV (or iCVV) or Card Authentication Method (CAM) authorization request cryptogram (ARQC) validation was not successful. Otherwise, this response code is reserved for Visa and Visa services.
		14	Invalid account number (no such number)	Yes	Used when following conditions occurs - • Account number was never issued or has been permanently blocked or closed, or • Failed Mod-10 check, or • Account number is not a valid length for issuer ***Note:*** *Not allowed for restricted transactions on valid accounts (use response codes in category 2)*
		15	No such issuer (first 8 digits of account number do not relate to an issuing identifier)	Yes	An issuer MUST not use this response code as it is reserved for Visa and Visa services.
		41	Lost card, pick up card (fraud account)		Use when a card has been marked as lost card and the credential has been reissued with a different PAN. Issuers should limit use to File Update messages (0302) from issuer to Visa.
		43	Stolen card, pick up (fraud account)		Use when a card has been marked as stolen card. Issuer should limit use to File Update messages (0302) from issuer to Visa.
		46	Closed account	Yes	Use for accounts closed by the issuer or the cardholder for any reason. PANs listed in the Visa exception file using response codes 04, 07, 41, or 43 must use this value.

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
		57	Transaction not permitted to cardholder	Yes	Limited use only. It should be used by issuer only if the condition applies to all PAN for the same product. It cannot be used for individual PAN to generically decline a transaction.
		R0	Stop this payment	Yes	Used when the cardholder requested to stop a specific single reoccurring payment transaction.
		R1	Stop all future payments	Yes	Used when the cardholder requested to stop all recurring payment transactions for a specific merchant account.
		R3	Stop all merchants	Yes	Used when all recurring payments have been cancelled for the card number in the request.
2	Allowed within threshold limit	**03**	Invalid merchant		Used when the issuer or cardholder has restricted (temporary or permanent) the card or product definition to not allow usage at Merchant Category Code (MCC).
		19	Re-enter transaction	Yes	Used when the issuer is temporarily unable to process a transaction due to an error in the message structure or field format or Address Verification failure. It is also used by Visa when a transaction exceeds the merchant fraud threshold designated in the Visa Transaction Advisor Service (e.g., at an automated fuel dispenser)
		51	Not sufficient funds		Used for debit and prepaid products when the cardholder does not have available funds or for credit products when the cardholder has reached the credit card limit. ***Note:*** *If the merchant has requested partial authorization, issuers can approve a lesser amount and use response code 10.*

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
		59	Suspected fraud	Yes	Used when a transaction fails a fraud rule in the issuers fraud detection system or Visa Real Time Decisioning (RTD)/Visa Risk Manager (VRM).
		61	Exceeds approval amount limit	Yes	It used by issuer when the defined amount activity limit for the account is exceeded. This is also used by Visa when • The issuer or acquirer settlement risk exposure cap has been exceeded or • The issuer defined velocity/amount limit for Original Credit Transaction (OCT) has been exceeded
		62	Restricted card (card invalid in region or country)	Yes	Used when a transaction is attempted from a country where transactions are restricted (temporary or permanent) including OFAC or embargoed countries.
		65	Exceeds withdrawal frequency limit		Used when the following conditions occur - • The defined count activity limit for the card or account (usually set daily) is exceeded, or • The transaction exceeds the Original Credit Transaction (OCT) withdrawal frequency limit if the issuer supports velocity checking
		75	Allowable number of PIN-entry tries exceeded		Used when the cardholder has entered an incorrect PIN multiple times. This may require additional risk investigations.

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
		78	Blocked, first used or special condition—new cardholder not activated, or card is temporarily blocked		Used when the following conditions occur – • A card has been issued but not yet activated (may trigger alert to cardholder), or • The account is temporarily blocked for all transactions due a special condition (e.g., delinquency or cardholder request)
		86	Cannot verify PIN	Yes	• Used by the issuer for system malfunctions for ATM transactions including hardware or processing system errors, or • Used in STIP when the issuer has not provided Visa with PIN verification keys or values
		91	Issuer unavailable or switch inoperative (STIP not applicable or available for this transaction) or Time-out when no STIP or Causes decline at POS.	Yes	Used when connectivity to the issuer system is unavailable and no stand-In instructions exist. The issuer, issuer processor, or STIP may respond to indicate that the authorization cannot be performed. When used by the issuer or issuer processor, this code does not cause STIP to be invoked. Use N0-Force STIP instead.
		93	Transaction cannot be completed, violation of law.		Used for regulatory restrictions which may be temporary or permanent. For example: • Gambling transactions • No 2nd Factor Authentication on domestic e-commerce transactions. Issuers should use 1A to describe this condition. There may temporary restrictions that are the result of regulation that can be fixed by the cardholder, such as the cardholder opting out of gambling, the cardholder opting out of e-commerce, etc.

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
		96	System malfunction	Yes	Used when following conditions occur – • Used to indicate that the issuer or issuer processor is unable perform the authorization due to system malfunction or critical message failure. • Used by Visa when errors in messaging are detected that prevent the message from being processed. • This code does not cause STIP to be invoked. Use N0-Force STIP instead.
		N3	Cash service not available		Used only for transactions involving cash or cashback and the issuer does not allow cash or cashback on the card requesting.
		N4	Cash request exceeds issuer or approved limit		Used only for transactions involving cashback and when the requested cashback amount exceeds the issuers limit for cashback at point of sale.
3	Allowed within threshold limit	**54**	Expired card or expiration date missing		Used when the authorization contains an expired or invalid or missing expiration date.
		55	PIN incorrect or missing		Used when the PIN fails the PIN verification process or is not present in the transaction when required.
		70	PIN data required		Used when PIN data is required and not present in the authorization request.
		82	Negative online CAM, dCVV, iCVV, CVV, CAVV, dCVV2, TAVV, or DTVV results		Used when a failure for CAM, dCVV, iCVV, CVV or service code within card present transactions.
		1A	Additional customer authentication required		Used only applicable for European based issuers for European merchants.

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
		N7	Decline for CVV2 failure		Used when a failure of CVV2 within card not present transactions. Do not decline CNP transactions for missing CVV2.
		01	Refer to card issuer		No longer permitted. Issuers are required to respond with either an approval or a descriptive decline response code. When no applicable response code is available in Category 1, 2 or 3, issuers may use other response codes defined in the Visa Technical specification however usage of these generic decline codes should remain minimal. ***Note:*** *The most used generic response code value is 05 Do Not Honor.*
4	Allowed within threshold limit	**02**	Refer to card issuer, special condition		Issuers are required to respond with either an approval or a descriptive decline response code. When no applicable response code is available in Category 1, 2 or 3, issuers may use other response codes defined in the Visa Technical specification however usage of these generic decline codes should remain minimal. Note: The most used generic response code value is 05 Do Not Honor. ***Note:*** *Response Code 13 may be used by issuers to decline Visa Direct OCT transactions for credit overpayment scenario.*
		05	Do not honor		
		06	Error (file update messages)	Yes	
		13	Invalid amount or currency conversion field overflow		
		39	No credit account		
		52	No checking account		
		53	No savings account		
		58	Transaction not allowed at terminal		
		64	Transaction does not fulfill AML requirement	Yes	

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Issuer Recommended Usage
		74	Different value than that used for PIN encryption errors		
		79	Reversed (by switch)		
		80	No financial impact (used in reversal responses to declined originals)		
		81	Cryptographic error found in PIN (used for cryptographic error condition found by security module during PIN decryption)	Yes	
		N0	Force STIP. issuers can respond with this, which routes transaction to STIP. Issuers use code when they cannot perform authorization but want STIP to perform it.		
		Z3	Unable to go online; offline-declined		

Table A–2: Response Code Details and Merchant/Acquirer Recommendations

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Merchant/Acquirer Recommended Action
Approval	Not Applicable	**00**	Approval and completed successfully		
		10	Partial approval		Ask for another payment mode/credentials for remaining amount.
Accepted	Not Applicable	**85**	No reason to decline a request for address verification, CVV2 verification, or credit voucher or merchandise return		
1	No reattempts allowed	**04**	Pick up card (no fraud)		• Reattempt not permitted for same PAN/Token • Ask for alternate payment method
		07	Pick up card, special condition (fraud account)		• Reattempt not permitted
		12	Invalid transaction	Yes	• Reattempt not permitted • Potential fraud is suspected or issues with merchant terminal • Review the following fields for possible failure conditions – Field 44.5—CVV/iCVV Results Code – Field 44.8—Card Authentication Results Code.
		14	Invalid account number (no such number)		• Reattempt not permitted with the same PAN or token • Revalidate account number for accuracy • Evaluate for potential fraud
		15	No such issuer (first 8 digits of account number do not relate to an issuing identifier)	Yes	• Reattempt not permitted with the same PAN or token • Revalidate account number for accuracy • Evaluate for potential fraud
		41	Lost card, pick up card (fraud account)		• Reattempt not permitted

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Merchant/Acquirer Recommended Action
		43	Stolen card, pick up (fraud account)		• Reattempt not permitted
		46	Closed account		• Reattempt not permitted with the same payment credential • Request alternate payment method from customer and/or advise the cardholder to contact their issuer
		57	Transaction not permitted to cardholder	Yes	• Reattempt not permitted with the same payment credential • Request alternate payment method from customer and/or advise the cardholder to contact their issuer
		R0	Stop this payment	Yes	• Reattempt not permitted • Contact customer regarding cancellation of all transaction from this merchant
		R1	Stop all future payments	Yes	• Reattempt not permitted • Contact customer regarding cancellation of all transaction from this merchant
		R3	Stop all merchants	Yes	• Reattempt not permitted • Contact customer regarding cancellation of all transaction from this merchant
2	Allowed within threshold limit	**03**	Invalid merchant		• Transaction should not be immediately reattempted for this merchant or MCC • Merchants and acquirers must not alter the merchant category code or other transaction data to gain approval

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Merchant/Acquirer Recommended Action
		19	Re-enter transaction	Yes	• If a merchant receives a high volume of RC19, contact acquirer to evaluate possible format errors • For Automated Fuel Dispenser, direct the cardholder to pay inside • Review the Field 44.2—Address Verification Result Code for possible failure
		51	Not sufficient funds		May reattempt for a lesser amount or at a later date to allow the customer to fund their debit account or pay down their credit account. ***Note:*** *Merchants can reduce NSF declines by implementing the Partial Authorization service*
		59	Suspected fraud		Advise the cardholder to contact their issuer and do not reattempt the transaction until the cardholder confirms.
		61	Exceeds approval amount limit	Yes	Do not reattempt the transaction the same day to allow limits to reset.
		62	Restricted card (card invalid in region or country)		Do not immediately reattempt. • Merchant may reattempt if the cardholder confirms the restriction has been removed • Merchants and acquirers must not alter country code or other transaction data to gain approval
		65	Exceeds withdrawal frequency limit		Do not reattempt the transaction the same day to allow limits to reset. • Merchant may advise the cardholder to contact their issuer

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Merchant/Acquirer Recommended Action
		75	Allowable number of PIN-entry tries exceeded		Do not reattempt the transaction the same day to allow limits to reset. • POS transactions may be reattempted as a non-PIN transaction if applicable
		78	Blocked, first used or special condition—new cardholder not activated, or card is temporarily blocked		Transaction should not be immediately reattempted. • Merchant may reattempt if the cardholder confirms the card has been activated or reactivated
		86	Cannot verify PIN		Reattempt can occur within same day. • POS transactions may be reattempted as a non-PIN transaction if applicable.
		91	Issuer unavailable or switch inoperative (STIP not applicable or available for this transaction) or Time-out when no STIP or causes decline at POS.		Reattempt can occur within same day. No more than one attempt per day.
		93	Transaction cannot be completed violation of law.		Do not reattempt
		96	System malfunction	Yes	Reattempt can occur within same day.
		N3	Cash service not available		Reattempt the transaction without the request for cash back.
		N4	Cash request exceeds issuer or approved limit		Declined transactions can be resubmitted with lower cashback amounts or actual purchase amount only.
3	Allowed within	**54**	Expired card or expiration date missing		• Validate the expiration date prior to reattempt • Monitor reattempts for potential fraud

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Merchant/Acquirer Recommended Action
	threshold limit	**55**	PIN incorrect or missing		• Reattempt with a valid value (re-enter PIN) • POS transactions may be reattempted as a non-PIN transaction if applicable
		70	PIN data required		• Reattempt with a valid PIN
		82	Negative online CAM, dCVV, iCVV, CVV, CAVV, dCVV2, TAVV, or DTVV results		• Review the following fields for possible failures and correct prior to reattempt – Field 44.5—CVV/iCVV Results Code – Field 44.8—Card Authentication Results Code. • Monitor reattempts for potential fraud
		1A	Additional customer authentication required		• For card present, reattempt using Chip + PIN • For card-not-present, reattempt transaction using 3D Secure
		N7	Decline for CVV2 failure		• Validate the CVV2 value prior to reattempt • Monitor reattempts for potential fraud
4	Allowed within threshold limit	**01**	Refer to card issuer		Reattempt allowed within the defined threshold limit and issuer is unlikely to provide an approval, as these are permanent conditions.
		02	Refer to card issuer, special condition		
		05	Do not honor		
		06	Error		
		13	Invalid amount or Currency conversion field overflow		
		39	No credit account		
		52	No checking account		
		53	No savings account		

Category	Reattempt Allowed?	Response Code	Definition	Used by Visa	Merchant/Acquirer Recommended Action
		58	Transaction not allowed at terminal		
		64	Transaction does not fulfill AML requirement		
		74	Different value than that used for PIN encryption errors		
		79	Reversed (by switch)		
		80	No financial impact (used in reversal responses to declined originals)		
		81	Cryptographic error found in PIN (used for cryptographic error condition found by security module during PIN decryption)		
		N0	Force STIP. Issuers can respond with this, which routes transaction to STIP. Issuers use code when they cannot perform authorization but want STIP to perform it.		
		Z3	Unable to go online; offline-declined		

Table A–3: Response Code Definitions

Response Code	Definition	Category
00	Approval and completed successfully	Approval
01	Refer to card issuer	4
02	Refer to card issuer, special condition	4
03	Invalid merchant	2
05	Do not honor	4
06	Error	4
10	Partial approval	Approval
12	Invalid transaction	Visa Reserved, 1
13	Invalid amount or Currency conversion field overflow	4
14	Invalid account number (no such number) or No Mod 10 check or Not a valid length for issuer or Not in positive PIN Verification file or Separator in wrong position	1
15	No such issuer (first 8 digits of account number do not relate to an issuing identifier)	Visa Reserved, 1
19	Re-enter transaction	2
39	No credit account	4
41	Lost card, pick up card (fraud account)	1
43	Stolen card, pick up (fraud account)	1
46	Closed account	1
51	Not sufficient funds	2
52	No checking account	4
53	No savings account	4
54	Expired card or expiration date missing	3
55	PIN incorrect or missing	3
57	Transaction not permitted to cardholder	Visa Reserved, 1
58	Transaction not allowed at terminal	4

Response Code	Definition	Category
59	Suspected fraud	2
61	Exceeds approval amount limit	2
62	Restricted card (card invalid in region or country)	2
64	Transaction does not fulfill AML requirement	4
65	Exceeds withdrawal frequency limit	2
70	PIN data required	3
74	Different value than that used for PIN encryption errors	4
75	Allowable number of PIN-entry tries exceeded	2
78	Blocked, first used or special condition—new cardholder not activated, or card is temporarily blocked	2
79	Reversed (by switch)	4
80	No financial impact (used in reversal responses to declined originals)	4
81	Cryptographic error found in PIN (used for cryptographic error condition found by security module during PIN decryption)	4
82	Negative online CAM, dCVV, iCVV, CVV, CAVV, dCVV2, TAVV, or DTVV results	3
85	No reason to decline a request for address verification, CVV2 verification, or credit voucher or merchandise return	N/A
86	Cannot verify PIN; for instance, no PVV	2
91	Issuer unavailable or switch inoperative (STIP not applicable or available for this transaction) or Time-out when no STIP or Causes decline at POS.	2
93	Transaction cannot be completed, violation of law.	2
96	System malfunction	2
04	Pick up card (no fraud)	1
07	Pick up card, special condition (fraud account)	1
1A	Additional customer authentication required	3
N0	Force STIP. Issuers can respond with this, which routes transaction to STIP. Issuers use code when they cannot perform authorization but want STIP to perform it.	4
N3	Cash service not available	2

Response Code	Definition	Category
N4	Cash request exceeds issuer or approved limit	2
N7	Decline for CVV2 failure	3
R0	Stop this payment	Visa Reserved, 1
R1	Stop all future payments	Visa Reserved, 1
R3	Stop all merchants	Visa Reserved, 1
Z3	Unable to go online; offline-declined	4

Table A–4: Field Level Details of a Message

Field Position	Message Data
Field 2	PAN or Token
Field 14	Expiry date YYMM
Field 22	Point-of-Service Entry Mode Code
Field 25	Point-of-Service Condition Code
Field 35	Track 2 Data
Field 44.2	Address Verification Results Codes
Field 44.3	Additional Token Response Information
Field 44.5	CVV/iCVV Results Code
Field 44.8	Card Authentication Results Code
Field 45	Track 1 Data
Field 52	Personal Identification Number (PIN) Data
Field 55	Integrated Circuit Card (ICC)-Related Data
Field 60.8	Mail/Phone/Electronic Commerce and Payment Indicator
Field 60.9	Cardholder ID Method Indicator
Field 63.3	Message Reason Code
Field 125	Original Transaction Identifier
Field 126.8	Transaction ID (XID)
Field 126.9	CAVV or TAVV Data
Field 126.10	CVV2 Authorization Request Data