Credit Voucher and Merchandise Return Authorization Messages – Global Implementation Guide

January 2019

Contents

1 Overview

From April 2018, acquirers and their merchants may optionally send credit voucher and merchandise return authorization transactions. Issuers must be prepared to receive and respond to authorization message for credit voucher and merchandise returns. Issuers are also required to update their online statements with the "pending" information, as they do with purchases. If issuers offer a text alert service to their cardholders for notification of purchases, this options must also be available to cardholders for purchase returns.

From October 2018, acquirers must be enabled to send and receive credit voucher and merchandise return authorization transactions to Visa. Credit voucher and merchandise return authorization transactions will be identified with a value of 20 (credit voucher or merchandise return authorization) in Field 3—Processing Code, positions 1–2 in authorization request (0100) message.

Acquirers and their merchants must support all valid approval response code values sent in Field 39—Response Code in authorization response (0110) message.

1.1 Audience

This guide is for Acquirers with respect to their implementation of purchase return authorization messages.

1.2 References

For more information, see the following documents, available on Visa Online.

- *New Purchase Return Authorization Messages Will Be Implemented - Visa Business News, dated 25 August 2016*
- *New Implementation Dates for Purchase Return Authorization Messages - Visa Business News, dated 20 July 2017*
- *Europe region: New Purchase Return Authorization Messages Will Be Implemented - Visa Business News, dated 12 January 2017*
- *Business Enhancement Release for April 2019 – Article 2.9, Mandate for Credit Vouchers and Merchandise Return Authorization Messages (earlier versions of the article, with the same titles, were included in the October 2017, April 2018 and October 2018 Business Enhancement Release documentation.)*
- *Purchase Return Requirements Will Be Updated in the Visa Rules – Visa Business News, dated March 8, 2018*
- *Implementation Date for Purchase Return Authorization Messages in the Visa Business News, dated 13 September 2018*
- *Visa Rules – Visa Core Rules and Visa Product and Service Rules (latest version)*

1.3 Terminology

In this document, Merchandise Return/Credit Voucher transactions will be referred to as Refunds or Refund transactions.

Merchandise Returns/Credit Vouchers are intended to address the return of funds to cardholders for merchandise and services returned to merchants. The initiative/mandate is NOT intended to address

the reversal or adjustment of Account Funding transactions. Account Funding and quasi-cash transactions are excluded from the mandate to send authorizations on merchandise returns/credit vouchers.

2 Benefits of return authorization messages

Authorization messages improve the flow of information on refunds by:

- Enabling issuers to update their cardholders' online banking statements in real time and provide text and/or mobile alerts to cardholders who opt in to the service with their issuer.
- Enabling issuers to identify unusual or suspected fraud activity sooner, as it is processed in real-time.
- Enhancing the information cardholders receive on purchase returns, aligning it with what they see on corresponding purchase transactions.
- Limiting acquirer research in tracking down refunds.
- Helping to reduce the number of customer service inquiries from cardholders to their issuer or the merchant related to the status of a credit.
- Timely information about refunds is expected help reduce the number of chargebacks related to 'credit not processed.'

Cardholder benefits

- Provides timely information regarding the status of funds being returned to their account
- Less likely to contact the merchant/issuer regarding status of credit

3 Refund processing overview

The following section provides operational recommendations to merchants for processing a refund. These options are listed in preferred order of action:

1. A merchant must first attempt to process the refund (credit transaction) to the same Visa account that was used for the original purchase transaction.
2. After proving that the original purchase transaction took place using a Visa account, a merchant may process the refund onto a different (alternate) Visa account under the following circumstances:
   - The original account is no longer available or valid (for example, the original card has been replaced due to expiration or being reported lost or stolen, or was a Visa Prepaid card that has since been discarded).
   - The authorization request for the refund transaction was declined by the issuer.
3. A merchant is permitted to offer an alternate form of credit (cash, check, in-store credit, prepaid card, etc.) when a refund cannot be processed to the original Visa account or to an alternate Visa account, because of one or more of the following conditions:
   - The cardholder does not have a receipt or other proof of purchase from the original sale.
   - The refund is made to a recipient of a gift (instead of to the cardholder who made the original purchase).
   - The original sale took place on a Visa Prepaid card, which has since been discarded.
   - The authorization request for the credit transaction was declined.

Additional considerations

Refunds to a Visa account are permitted only when a Visa account was used to make the original purchase. For example, if the original purchase was made with a non-Visa method, such as cash or a non-Visa general purpose payment card, the merchant should not credit a Visa account, unless it is submitted as an 'original credit' transaction. There is no longer any requirement for a merchant to identify the original sale on a refund transaction receipt.

None of these requirements affect a merchant's ability to establish its own refund/return policy, which includes the ability to refuse or restrict refunds, returns, cancellations or exchanges, provided that the policy complies with applicable law and is disclosed to the customer at the point and time of purchase as defined in the *Visa Rules - ID#: 0008771*.

4 Merchant acceptance requirements

The requirements outlined in this section apply to the following acceptance channels:

Data Capture Method	Device Types / Acceptance Channel
PAN Key Entered	Attended POS, E-Commerce, M-Commerce, MOTO (CNP)
Card on File	MOTO, E-Commerce, M-Commerce
Mobile Wallet (EMV)	In-App, M-Commerce
Magnetic Stripe	Attended POS, mPOS
Contact Chip	Attended POS, mPOS
Contactless	Attended POS, mPOS
Original Purchase Transaction Recall (Cardholder may be present but card not used)	Attended POS, mPOS, MOTO, E-commerce, M-commerce, In-App

4.1 Return Authorization Messages

All refund transactions must be authorized online regardless of any transaction floor limits that may exist for purchase transactions. Failure to submit refund authorization requests will be monitored under the Visa Rules compliance program and may result in non-compliance fines being imposed on the merchant acquirer.

If, due to operating restrictions, the merchant or its acquirer is unable to submit authorization requests for a period of time, it is recommended that outstanding requests are submitted as deferred authorizations as soon as the operating restriction has been removed.

4.2 Authentication Data and POS Entry Mode

Merchants can initiate the return by swiping, dipping or tapping the Visa card or by scanning the original purchase receipt. Merchants must send the POS entry mode and authentication data that are applicable to the return transaction and must not include additional data from the original transaction (such as partial track data or cryptogram) from the original transaction.

4.2.1 Contact or Contactless EMV Chip Data

If full EMV Chip cryptographic data is captured by the merchant terminal at the time of the refund (and processed/included in the authorization message), the value of the POS Entry Mode (field 22, positions 1-2) must contain the value of either **05** or **07** for either contact or contactless entry mode, as appropriate.

If only PAN and expiry date are sent in the refund transaction (for example, in transaction recall/scanning of original receipt scenarios), POS entry mode **01** is recommended regardless of the POS Entry Mode/capture method of the original purchase transaction.

4.2.2 PAN Key Entered or Card On File Transaction

For PAN Key Entered or Card on File transactions, CVV2, Verified by Visa (VbV) Data or Address Verification Data is not required but will be validated in the transaction data submission, if captured. The value of the POS Entry Mode (field 22, positions 1-2) must contain the value of **01** If CVV2 data is not obtained from the cardholder, do not send CVV2 field data (do not send F126.10).

4.2.3 Scanned Receipt (card is not dipped/tapped/swiped)

Refund transactions performed using recalled transaction data from the original purchase are recommended to only use the minimum data requirements of PAN and Expiry Date for the credit authorization request. The inclusion of partial track data or recalled full EMV chip cryptographic data may cause the authorization request to be declined by the card issuer, as this may be seen as a fraudulent use of the original transaction data (such as scanning a receipt); In the event of a scanned receipt (card is not dipped/tapped/swiped), POS entry mode **01** is recommended. It is important to understand that a refund/merchandise return is a stand-alone transaction (not part of a transaction "set") and does not require original transaction data, as this could lead to an unnecessary decline.

4.3 Cardholder Verification

Verification of the identity of the cardholder by requesting a PIN or capturing a signature is not required for this type of transaction, but may be carried out if required by existing merchant policies or procedures for conducting merchandise returns.

4.4 Response to the Authorization Request

Merchant acquirers, processors, merchant systems and all Point of Sale devices and terminals must be capable of receiving and correctly acting on any response returned by the card issuer or the Visa stand-in processing (STIP) service in field 39 of the authorization response (0110) message.

4.4.1 Approval Responses

Response codes **00 - approval** and **85 – no reason to decline** must be actioned as an approval response from the card issuer by the merchant.

4.4.2 Decline Responses

Issuers are encouraged to approve refund authorizations for all valid account numbers. However, the card issuer may decline the refund authorization request for a number of reasons. If the point of sale terminal provides the specific reason for the decline, the merchant can provide an appropriate customer message on how to proceed to ensure a positive cardholder experience. Below are commonly received response codes and recommended actions that a merchant can take to complete the transaction.

Response Code(s)	Description	Suggested Merchant Action
00, 85	Approve/ No Reason to decline	No additional action required, the refund has been approved.
14	Invalid Account Number or Account Type	Indicate that the account for this card is not recognised and request alternative Visa Card to perform the refund or, if this is not available, perform refund using another method (refer to Section 3).
39, 52, 53	Invalid Account Type	Verify that the cardholder has selected the correct account type (credit or debit) on the POS device
54	Card Expired	Indicate that this card is expired and ask the cardholder if a replacement card is available to re-perform the refund. Otherwise ask for an alternative Visa Card or, if this is not available, perform the refund using another method (refer to Section 3).
55	Invalid PIN	Perform normal Online PIN re-try processing. (If this refund transaction was declined upon retrying with the PIN, refer to Section 3.)
All other decline codes	Declined	Ask for an alternative Visa Card or, if this is not available, perform the refund using another method (refer to Section 3).

4.5 Completing the transaction

The Authorization Identification Response (6-digit approval code) returned by the issuer (VisaNet message field 38) in the authorization response message must be included in the credit transaction clearing record.

4.5.1 Receipt requirements

The transaction receipt requirements are listed in Table 5-34 in Section 5.10.3.2 of the April 2018 version of the Visa Core Rules manual. Purchase returns should follow the same requirements as other authorization requirements, such as including the Authorization Code on the receipt, as merchants do today for purchases. Since receipts have already been required for returns, please ensure that the authorization code response received from the issuer is printed on the receipt, as it is today for purchase transaction receipts. Some of the other required elements include the masked Account Number/Payment Token, Card Network Name, and Transaction Type. The full list, along with the additional requirements, can be found in the above-mentioned table.

4.5.2 Validating signature

Unless local regulations require this to be performed, there is no Visa requirement to validate the cardholder for a refund transaction to complete successfully.

If the merchant is required to validate the cardholder using signature validation, then the normal processing rules for this cardholder verification method apply.

5 VisaNet messaging requirements

For more information on the fields and values in credit voucher and merchandise return authorization transactions, refer to:

- *BASE I Technical Specifications, Volume 1 and Volume 2*
- *SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1 and Volume 2*

Authorization Field Requirements

Following are the mandatory, minimum fields required in a Card-Not-Present and Card Present transaction:

Request Message 0100		**Response Message 0110**	
Field	**Content**	**Field**	**Content**
2	Primary Account Number (PAN)	2	Primary Account Number (PAN)
3	Processing Code - First 2 positions sent with a value (Transaction Type) of 20	3	Processing Code - First 2 positions with a value (Transaction Type) of 20
4	Transaction amount (amount of return)	4	Transaction amount (amount of return)
7	Transmission date and time	7	Transmission date and time
11	System Trace Audit Number	11	System Trace Audit Number
18	Merchant Type (MCC)		
19	Acquiring Institution Country Code	19	Acquiring Institution Country Code
22	Point-of-Service (POS) Entry Mode Code		
25	Point-of-Service (POS) Condition Code	25	Point-of-Service (POS) Condition Code
32	Acquiring Institution Identification Code	32	Acquiring Institution Identification Code
35*	Track 2 Data		
37	Retrieval Reference Number	37	Retrieval Reference Number
		38	Authorization ID Response
		39	Response Code
42	Card Acceptor Identification Code	42	Card Acceptor Identification Code
43	Card Acceptor Name/Location		
45*	Track 1 Data		
49	Currency Code, Transaction	49	Currency Code, Transaction

Request Message 0100		Response Message 0110	
55*	Chip Card Data	55*	Chip Card Data
62.1	Authorization Characteristics Indicator - Acquirers should send a value of Y in F62.1	62.1	Authorization Characteristics Indicator - [Issuers/issuer processors should receive a response value of T in F62.1]
63.1	Network Identification Code	63.1	Network Identification Code
126.10	CVV2 Authorization Request Data		

*only in a Card Present environment where cardholder has been asked to swipe or dip card for refund

The "Card Expiry Date" is strongly recommended for both Card Present and Card-Not-Present transactions. Although Card Expiry Date is not a mandatory field in the credit voucher and merchandise return authorization message, some issuers may choose to decline any authorization request for an expired or missing expiration date. It is a best practice to include a valid expiration date in the authorization request message, if at all possible. If a merchant is processing an authorization for a refund to a since expired card, best practice is to omit Field 14 (Date, Expiration) from the message (for Card Not Present transactions.)

Clearing Record Requirements

With the implementation of authorizations on purchase returns, acquirers must carry over key data elements from the 0110 responses into the clearing record. (This is in addition to the fields acquirers pass today.) The key fields that are required are the Authorization Identification Response Code and the Transaction Identifier.

From:	To:
Authorization Response 0110	Transaction Code – TC06
Authorization Identification Response - field 38 (6 position Alpha/Numeric)	TCR 0 record - Authorization Code - positions 152 - 157
Transaction Identifier - field 62.2 (15 Numeric; 8 bytes, right-justified)	TCR 5 record - Transaction Identifier - positions 5 - 19

5.1 Additional notes

- Merchandise Return/Credit Voucher/Refund transactions are standalone transactions (not part of a transaction "set," in the same way that an authorization, a reversal and related chargebacks are all part of a transaction "set." They do not reference a former transaction (for example, Fields 11 System Trace Audit Number, 37 Retrieval Reference Number, and 62.2 Transaction Identifier do not match between authorization and merchandise return/credit voucher/refund).
- Although these authorizations are not Custom Payment Service (CPS) transactions, acquirers that participate in CPS must submit the value of **Y** (Transaction requests participation) in Field 62.1—Authorization Characteristics Indicator (Bitmap Format). V.I.P will then overlay the value of **Y** with the value of **T** (No CPS program is available) before forwarding the message to issuer processors.
- Transaction Identifier Field 62.2 is added by VisaNet in the 0100 request message to the issuer and is included in the 0110 response to the acquirer.

5.1.1 In-Store Scanned Receipt Refund Transactions

- A POS Entry Mode of **01** is recommended for transaction data recall/scanned receipt refund scenarios, where a card is not swiped/dipped, or device not tapped, at POS for the refund.
  - In this scenario, the merchant simply refunds the original form of payment, without asking the cardholder to re-present their card/device.
- This will ensure PAN and expiry date are the minimum requirements for issuer to approve
- Leads to higher approval rates as some issuers may decline transactions if the POS indicator is inconsistent with the data being provided. An example of this would be if the merchant indicated that the transaction was chip read but there was not a cryptogram provided.
- While some merchants can recall the cardholder's credentials when processing a refund (e.g. scanned receipt), Visa does not view these as "Credential on File" transaction. The "Credential on File" POS Entry Mode value of 10 is intended for transactions where payment credentials were explicitly stored for future use.

Note: If the cardholder is asked to swipe/dip their card, or tap their device, at the time of refund (after the merchant scans the original receipt) then the normal transaction data applicable for these POS transactions applies (for example, sending POS EM 05 and Field 55 CHIP data if the card is dipped for the return).

5.1.2 Reversals

Message Type: 0400/0410/0420/0430

Description: Credit Voucher and Merchandise Return Authorization Reversal, Issuer STIP Advice, Issuer Switch Advice, and Responses

Reversals of merchandise return transactions are valid with Processing Code 20 (positions 1-2). However, a Processing Code of 20 should never be used in reversals of authorizations/purchases (when not specifically reversing a merchandise return).

5.1.3 Reversal Scenarios

Scenario 1: If a merchant sent a refund in error and needs to void the return, the best practice is to send an 0400 to reverse the refund authorization.

Scenario 2: If the response to the merchandise return message cannot be sent back to the merchant terminal, an acquirer reversal will be generated. The acquirer should send an 0400 reversal message type with Processing Code 20 to Visa.

5.2 Chip data fields

Issuers must be prepared to support all fields and values in credit voucher and merchandise return authorization messages submitted by acquirers and merchants. The credit voucher and merchandise return authorization messages may or may not contain chip data. However, if chip data is present, any cryptogram type may be present and must not impact whether the refund is approved or declined.

6 Authentication

The values used to populate the authorization message must be consistent with the documentation provided by Visa technical manuals. Merchants can obtain the cardholders' credentials in a variety of ways, such as accessing the store's transaction history, using the transaction receipt for reference. Alternatively, the merchant can obtain the account number through more common means, such as reading the account number off of the chip, mag stripe, or reading/keying the account number off the information on the card. However they are obtained, the POS entry mode must be correctly identified based on Visa technical documentation. If a merchant indicates that the POS entry mode is **05**, indicating EMV, they would need to include the chip data in field 55. If the account number is obtained from the chip but the merchant/acquirer does not want to pass the field 55 data, they should use the POS entry mode of key-entered (01), so that the issuer does not try to validate chip data that is not present.

The PAN and expiry date should be used to perform the refund. Chip data is not required in the online refund message, as it is an optional field that may be populated, but is not required in order to complete the refund. If you choose to populate this field, the AAC received from the card can be populated in the message. You may use the PIN bypass (or selectable kernel) if it simplifies the processing on the terminal. However, for debit it is highly recommended that the same PIN process used for your normal transaction flow is followed in order to keep the Terminal flows the same between a transaction and a refund and to comply with your online switching requirements (specifically with regards to common debit routing in the US). More importantly, PIN may be required on certain networks.

It is important to note, acquirers should use the POS entry mode that corresponds to what is being sent. If a card is not dipped, for example (and chip data is not being captured with the refund transaction), do not send a POS Entry Mode of **05** (likewise for contactless transactions with POS EM 07). If chip data is present, note that the specific cryptogram type is irrelevant to the transaction. This may be an application authentication cryptogram (AAC), authorization request cryptogram (ARQC), or transaction code (TC).

For EMV/chip authorizations, any cryptogram type is acceptable (AAC, ARQC, TC). If you have chip data, clients should send this. An AAC implies no transaction performed at chip level. This should be consistent with purchase authorizations. For a sale this would indicate a decline, but not for a refund. This is more to do with the correct handling of offline counters and limits on the card. In the case of a refund, it is specifically documented to be an AAC. The AAC can still be validated by the issuer in the same manner as any other cryptogram. The issuer has the choice to validate or ignore.

7 Certification and implementation testing

Acquirers must modify their systems to send credit voucher and merchandise return authorization transactions to Visa. There are no activation requirements with Visa for this enhancement.

Test transactions are available in the Visa Test System. Acquirers are highly recommended to test in order to run through the various purchase return scenarios to ensure minimal declines. Testing can begin at any time.

Implementation Summary

System/Service	Acquirers	Change
V.I.P. Authorization Only	X	Acquirers must modify their systems to send credit voucher and merchandise return authorization transactions to Visa [according to the schedule in Table 2.7.A of the Technical Letter]