Visa Europe

# Dual Message System Authorization (DMSA) Processing Specifications

June 2015

# Contents

# Tables

# Figures

# 1 Introduction

The *Dual Message System Authorization (DMSA) Processing Specifications* describe the processing requirements and options for the DMSA component of the Visa Europe Authorization Service (VEAS).

## 1.1 Audience

This manual is for Members' technical staff, managers, Business Services Support, and customer support personnel who help Members solve system and production problems.

## 1.2 Purpose

This manual provides Members and their Processors with an overview of DMSA and comprehensive information about DMSA message processing.

## 1.3 Scope

This manual provides an overview of DMSA and comprehensive information about DMSA message processing, including:

- Message types
- Message flows for both authorization and non-authorization messages
- Initial message parsing and editing
- Message processing
- Message routing
- Stand-in processing (STIP)

This manual is designed to be used in conjunction with the *Dual Message System Authorization (DMSA) Technical Specifications*.

## 1.4 Summary of changes

The following highlights revisions made to the *Dual Message System Authorization (DMSA) Processing Specifications*:

- Reformatted to new corporate presentation standards
- Fully revised throughout

## 1.5 Document conventions

The following conventions are used throughout this guide.

### 1.5.1 Formatting and style

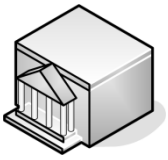
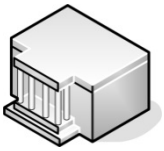
The following conventions apply to formatting and style throughout this guide:

- Words that are displayed with initial capitalisation have a special definition beyond, or in lieu of, their dictionary meaning. For the complete list of Visa Europe defined terms, refer to the *Visa Europe Operating Regulations*.

- Words that are displayed with initial capitalisation and are not specified as defined terms or written in italics, are proper nouns used within the Visa Europe and Member environments, for example:
  - Names of services, processes and entities specific to Visa Europe or Visa Europe Members
  - Names of Visa Europe departments
  - Names of options
  - Names of files
  - Titles of reports
- **Bold** type is used for visual emphasis.
- References to other publications and to sections within the document are in *italics*.

### 1.5.2 Diagrammatic conventions

The following conventions apply to diagrams throughout this guide:

| | |
|---|---|
|  | Indicates an Acquirer |
|  | Indicates a Visa Europe component, for example, VEAS or VECSS |
|  | Indicates an Issuer |
| **Request** | Indicates a request message |
| **Response** | Indicates a response message |
| **Advice** | Indicates an advice message |
| **Advice Response** | Indicates an advice response message |
| **TC *nn*** | Indicates a transaction by a translation code (TC) and used during clearing and settlement |

## 1.6 Related information

The following publications provide information related to the *Dual Message System Authorization (DMSA) Processing Specifications*.

### Visa Europe technical overviews

- *Introducing the Visa Europe Authorization Service*
- *Introducing the Visa Europe System*
- *Introducing Dual Message System Clearing (DMSC) Transactions*
- *Introducing Dual Message System Clearing (DMSC) Messages*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Messages*

### Visa Europe service descriptions

- *Visa Europe Technical Service Descriptions*

### Visa Europe technical and processing specifications

- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Single Message System (SMS) ATM Technical Specifications*
- *Single Message System (SMS) POS Technical Specifications*
- *Single Message System (SMS) ATM Processing Specifications*
- *Single Message System (SMS) POS Processing Specifications*
- *Single Message System (SMS) and Dual Message System Authorization (DMSA) Reports*
- *Dual Message System Clearing (DMSC) Technical Specifications*
- *Visa Europe System Management for Members*

### Visa Extended Access Server (EA Server) manuals

The Visa Inc. documentation is used; there is no Visa Europe equivalent. For information about Extended Access Server manuals, please contact eunetworksupport@visa.com.

### Miscellaneous publications

- *Payment Technology Standards Manual*
- *Card Recovery Bulletin Service User's Guide*
- *Authorization Gateway Service Cross-Reference Guide*
- *Visa Europe Operating Regulations*
- *Visa Smart Debit/Credit System Technical Manual*
- *Visa Money Transfer Global Implementation Guide*
- *International Organization for Standardization (ISO) 8583; 1987 (E): Bank Card Organizational Messages - Interchange Message Specifications - Content for Financial Transactions*

For summary information on all Visa Europe services, refer to *Introducing Visa Europe Services*. See also the *Visa Acronyms Quick Reference* document for a list of Visa acronyms and abbreviations and their meanings.

For further information, you can also visit our website via the following links or contact Visa Europe Customer Support:

- For information about Visa Europe: www.visaeurope.com
- For Member documentation: www.eu.visaonline.com

## 1.7 Feedback

If you have questions or comments about this document, please send them to: customersupport@visa.com

# 2 Overview of DMSA and the Visa Europe System

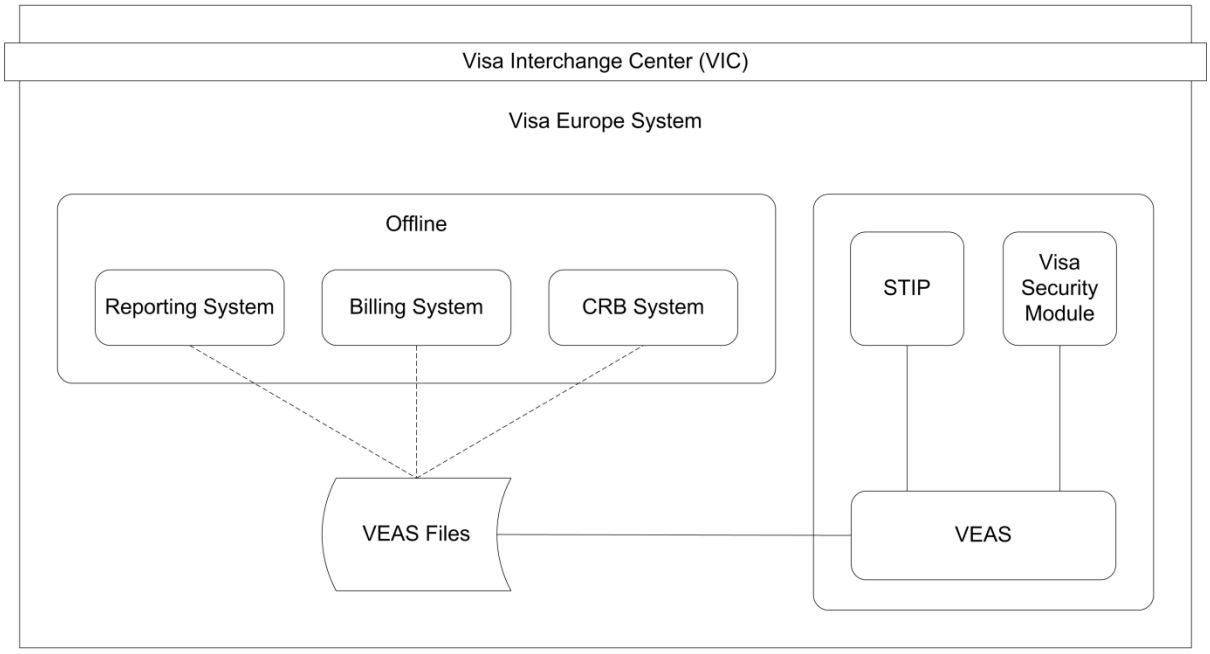
Understanding DMSA requires a basic understanding of the Visa Europe System and the interaction of its system components. This chapter contains information that provides a foundation for understanding the DMSA information in this manual, including:

- A brief description of the Visa Europe System and its major components
- An overview of DMSA online functions and offline functions

For an overview of the Visa Europe System and of the Visa Europe Authorization Service (VEAS), refer to *Introducing the Visa Europe System* and *Introducing the Visa Europe Authorization Service* respectively.

Figure 1 illustrates the DMSA software components and the system tables used for online and offline functions.

**Figure 1: DMSA software and files**




## 2.1 Visa Europe System components

The Visa Europe System is the primary interface for Cardholder transactions that originate within the Visa Europe Territory (the extent of the Territory is defined in the *Visa Europe Operating Regulations*). It is interoperable with VisaNet, the primary interface for all transactions that occur outside the Territory, ensuring that Cards can be used throughout the world irrespective of their country of issuance. The term Visa Europe System applies to the Territory's hardware, software, and communications components and facilities.

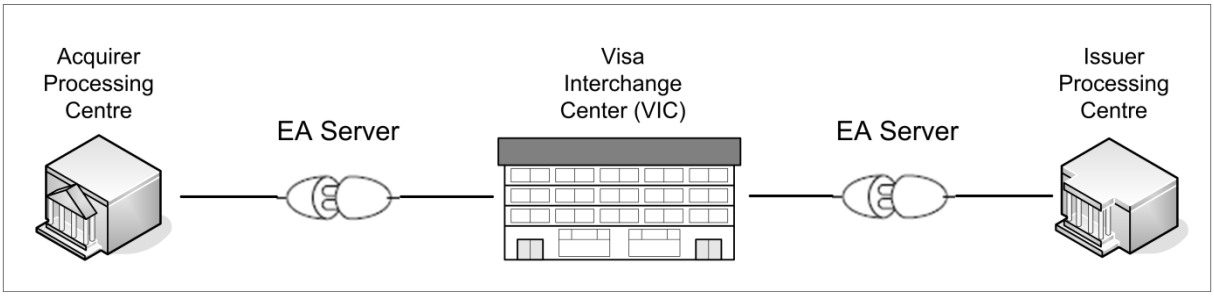
The main components of the Visa Europe System are:

- Visa Interchange Centers (VICs)
- Visa System communications network
- Visa Europe access points, via a Visa Extended Access Server (EA Server) or Direct Exchange (DEX)

- Processing Centres

Figure 2 illustrates the traditional Visa Europe System, with an EA Server in place for each Member. DMSA is a subset of VEAS, which is part of the Visa Europe System.

**Figure 2: The Visa Europe System communications network**




### 2.1.1 Visa Interchange Centers

A VIC operates the Visa data processing systems and support networks. Visa operates four VICs: two in the US and two in the UK. The VICs in the US run systems managed by Visa Inc., including the V.I.P. System. The VICs in the UK run systems managed by Visa Europe, including VEAS.

Each VIC houses the computer systems that perform all Visa Europe System transaction processing and serves as the control point for the telecommunications facilities of the Visa System communications network. The Visa Europe System connects Members to the closest VIC. If one VIC experiences system disturbances that interrupt system processing, the Visa Europe System automatically routes Members' transactions to another VIC, ensuring continuity of service.

Both VICs in the UK house DMSA as a component of VEAS, the main Visa Europe transaction processing system. The Single Message System (SMS) is also a software component of VEAS.

### 2.1.2 Communication networks

Visa operates telecommunications lines and facilities worldwide to link all systems users to the VICs and thus to each other. Most links in the Visa System communications network are high-speed leased lines; other links use satellite connections.

Almost all communications are based on IBM SNA and TCP/IP conventions and protocols.

### 2.1.3 Access points

Visa Europe provides access points for connecting to the Visa Europe System. These enable Members to connect to the Visa Europe System for transaction processing. Access points include:

- Visa Extended Access Server

  The EA Server is based on open systems technology and on a hardened Solaris operating system. Each EA Server is located at the participating access point site. The servers perform authorization routing, file staging, and delivery services, and provide secure connectivity to the Visa Europe System.

  An EA Server allows accessibility and flexibility, thereby enabling easy deployment for future Visa Europe product and service offerings, as well as other customisation. Their

modular interface adapts to front-end systems and integrates standard, off-the-shelf components that Members can scale to meet specific service needs.

- Direct Exchange (DEX)

  The Visa Direct Exchange (DEX) network provides Members with a single network access point for all message processing and file delivery services.

  The DEX network has two major components:

  - The Visa Message Gateway, which handles online transaction processing, resides at the VIC and supports all VEAS messages. The Visa Message Gateway operates as a routing switch for all VEAS transactions processed through it, controls the flow of traffic between access points and the VIC, and effectively replaces the EA Server in end-to-end DMSA and SMS online processing.
  - The Open File Delivery (OFD) Service, which handles report and file delivery, including the delivery of Automated Clearing House (ACH) data, DMSC data, the Point-of-Sale Authorization (POSA) File, and various reports and raw data.

Members can choose additional options for receiving reports and raw data and for routing files.

Options vary by region. Members can contact their Visa Europe Customer Support for information about available connectivity options.

### 2.1.4 Processing Centres

A Processing Centre, often called a Processor, is a data processing facility operated by or designated by an Issuer or an Acquirer. The Processing Centre houses Card processing systems that support Merchant and business locations, maintain Cardholder data and billing systems, or both. Each Processing Centre host computer that communicates with an EA Server must run a computer interface to the EA Server. Visa Europe must certify this interface before the EA Server can be connected to the Visa Europe System.

## 2.2 Visa Europe System transaction processing

The main transaction processing systems within the Visa Europe System that provide online and offline transaction processing are:

- VEAS, which includes:
  - The Dual Message System Authorization (DMSA)
  - The Single Message System (SMS)
- Visa Europe Clearing and Settlement System (VECSS), which includes:
  - The Dual Message System Clearing (DMSC)
  - The Visa Europe Settlement Service (VSS)

The following subsections describe each of these systems.

### 2.2.1 Visa Europe Authorization Service

VEAS is the primary online transaction routing (switching) and processing system for all online authorization and financial request transactions that enter the Visa Europe System. The

system provides the authorization services described in this manual to Members and to other users worldwide.

VEAS has one system that supports dual-message processing (Members request authorization of transactions in a first message, then send financial clearing information in a second message), and another system that supports single-message processing (the processing of transactions that contain both authorization and clearing information in a single message). In both cases, settlement occurs separately.

### 2.2.2 Floor Limit

A Merchant's Floor Limit is an amount limit set by the Acquirer (subject to *Visa Europe Operating Regulations* maximums) that determines if the transaction requires VEAS for completion. Transactions at or below the Floor Limit do not require authorization processing, although VEAS will process authorizations of any value that Merchants send.

**Important** Merchants choosing not to seek online authorization must check the Card Recovery Bulletins (CRBs) to ensure that the account is not listed. If the Merchant does not perform this check and it is later determined that the account or the Cardholder was in fact listed in the CRB, the Merchant is liable for Chargeback fees.

The maximum Floor Limit for most Cash Disbursements is zero, meaning that the Issuer or STIP must always authorize these transactions.

Visa continually evaluates Floor Limits to minimise Members' risk; refer to the *Visa Europe Operating Regulations* for details. Members are notified of Floor Limit changes that occur between releases of the *Visa Europe Operating Regulations* by Visa Europe Member Letter.

### 2.2.3 Dual Message System Authorization

DMSA is the component of VEAS that processes authorization-only request messages online. Authorization Request messages are the first messages sent in dual-message processing. (DMSC clearing messages are the second messages sent in dual-message processing.)

The DMSA component of VEAS supports online functions, offline functions, and the DMSA files. DMSA files include the internal system tables and the Cardholder Database (CDB).

For information about the Cardholder Database, refer to *System Management for Members*.

### 2.2.4 Single Message System

The SMS component of VEAS processes full financial transactions. Full financial transactions contain both authorization and clearing information.

Because one message contains both the authorization and clearing information, this form of processing is referred to as single-message processing. SMS also supports dual-message processing (participants submit an Authorization Request as a first message, then send clearing and settlement in a second financial request message), communicating with DMSA, and accessing outside networks, as required, to complete transaction processing. Only the SMS component performs single-message processing.

A bridge from SMS to DMSA makes it possible for SMS users to communicate with DMSA users and to access the DMSA gateways to outside networks.

SMS supports online functions, offline functions, and SMS files. SMS files consist of internal system tables that control system access and processing, and the Cardholder Database, which contains files of Cardholder data that VEAS uses for authorization.

### 2.2.5 Dual Message System Clearing

DMSC is an international electronic batch transaction clearing system that facilitates the exchange of Interchange data between Acquirers and Issuers. The system calculates Interchange Reimbursement Fees (IRF) between Members.

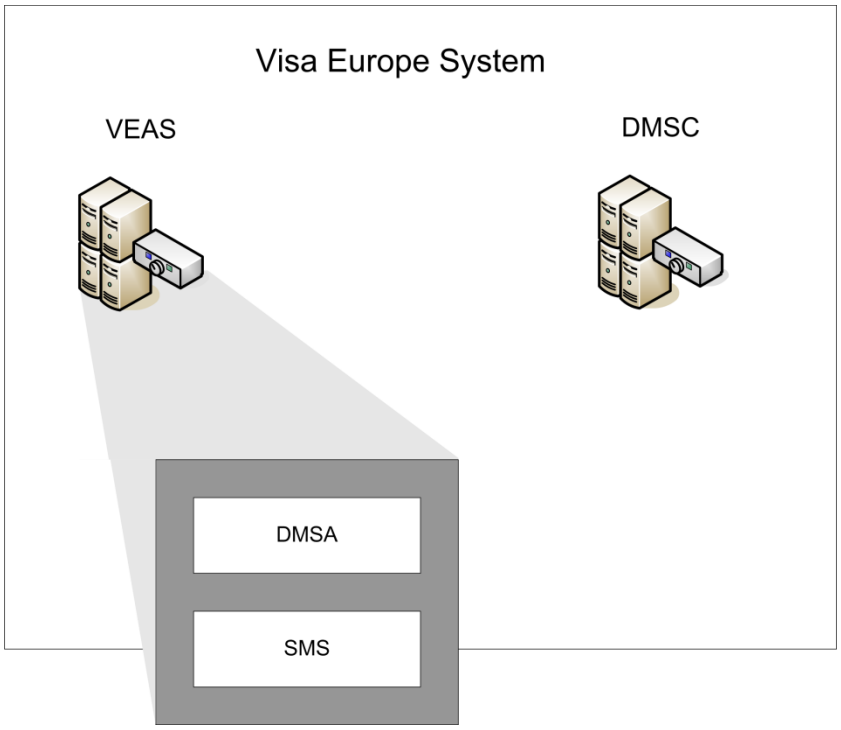
DMSC performs the second part of dual-message processing. Through a DMSA or SMS connection, Members submit authorization messages, which VEAS clears through a Visa Europe System connection to DMSC. A bridge to VEAS permits Interchange between Processing Centres for DMSC and those for SMS.

**Note** This manual does not provide details about DMSC. For information about this system, refer to the DMSC documents listed in Section 1.6, *Related information*.

Settlement occurs through VSS. DMSC passes message data to VSS, which settles with the Issuer and with the Acquirer. See Section 2.2.6, *Visa Europe Settlement Service*, for information about VSS.

Figure 3 illustrates where VEAS and its software system components, along with DMSC, reside in the Visa Europe System.

**Figure 3: Visa Europe System software system components**




Members and Processors that use DMSA and DMSC may choose to use SMS to process some of their transactions, or may choose to use different processing methods for different transaction types.

**Example:**

An Issuer can use DMSA and DMSC processing for POS transactions and use SMS processing for ATM Transactions.

### 2.2.6 Visa Europe Settlement Service

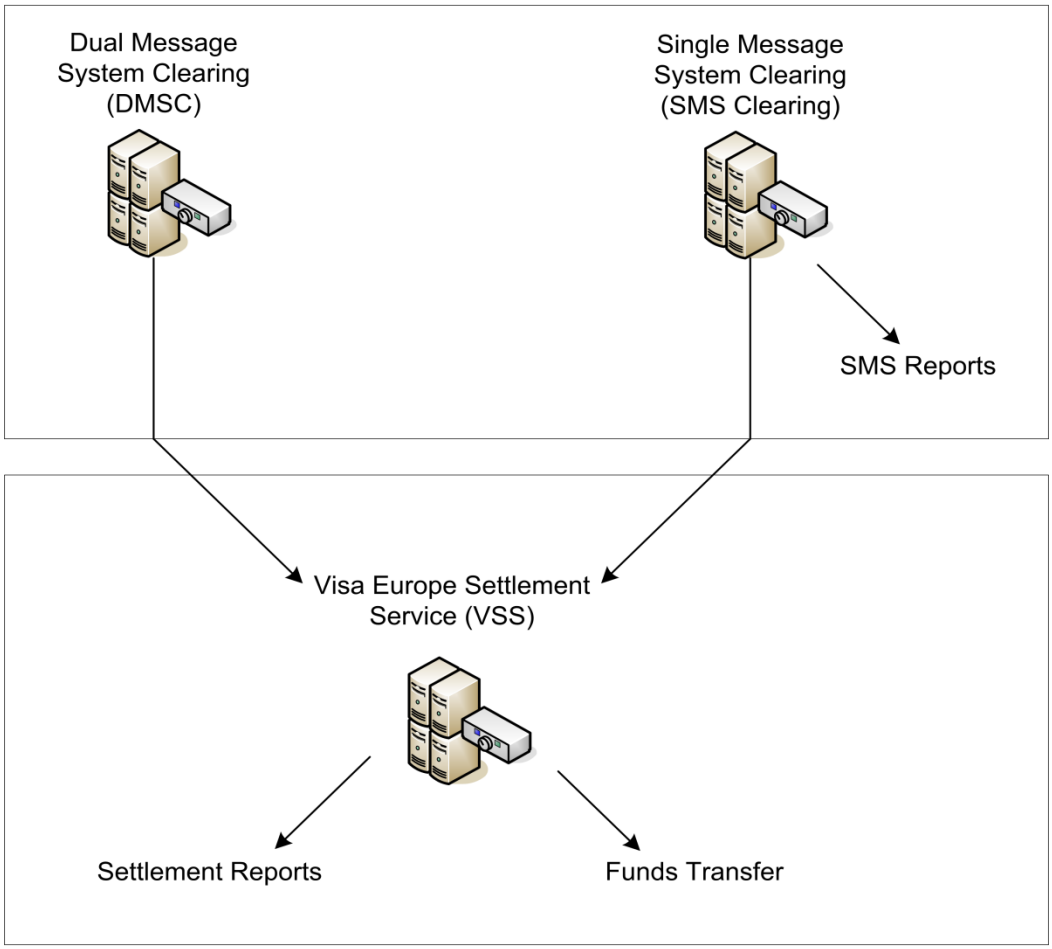
The Visa Europe System processes Interchange transactions for SMS and for DMSC through separate systems. Both SMS and DMSC perform their own clearing functions. Clearing is the process of collecting an individual transaction from one Member or Processor and delivering it to another. Clearing also includes valuation, the calculation of many types of fees and charges.

Once the systems clear transactions, they are ready for settlement. Settlement is the process of calculating and determining the net financial position of each Member for all transactions that the Visa Europe System clears.

VSS consolidates the settlement functions of SMS and DMSC, into a single service for all products and services. The Visa Europe System sends the settlement information to Members and Processors from SMS and from DMSC in a standardised set of reports. VSS provides flexibility in defining financial relationships, in selecting reports and report destinations, and in establishing funds transfer points.

Figure 4 illustrates how VSS fits into the Visa Europe Clearing and Settlement Service (VECSS) process.

**Figure 4: Visa Europe Clearing and Settlement Service (VECSS) process**

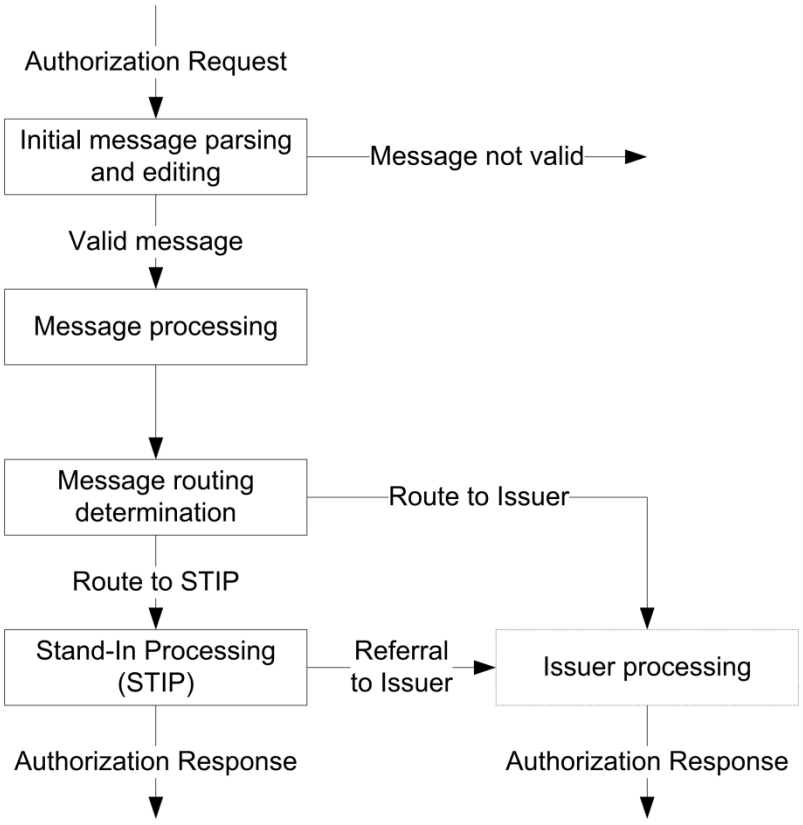


## 2.3 DMSA online functions

The DMSA online functions support dual-message authorization processing. DMSA online functions include processing of Authorization Requests from Cardholders, authorization reversals and the generation of advices. As shown in Figure 5 online authorization functions include:

- Initial message parsing and editing
- Message processing (such as risk determination, PIN verification, and Chip authentication)
- Message routing
- Stand-in processing

**Figure 5: DMSA message preparation, routing, and STIP**




### Types of transaction

How DMSA routes and processes a transaction depends on:

- The type of Card used
- The processing network preferred by the Acquirer
- The type of Acquirer, DMSA - Issuer is either DMSA or SMS
- The type of message used to request processing of the transaction, either authorization or financial
- The type of Processing Centre used by the Issuer, DMSA - Acquirer is either DMSA or SMS

A bridge from DMSA to SMS makes it possible for DMSA Members to communicate with SMS Members and to access the SMS gateways to outside networks.

For information about outside networks supported by Authorization Gateway Services, contact Visa Europe Customer Support.

### Processing rules

For each Card transaction, Members and Processors connect to DMSA using V.I.P. processing rules (for further details, see Section 4.1.1, *BASE I and V.I.P. alignment - Background*.)

### Cardholder activities

Depending on the processing rules and on the type of transaction, DMSA supplies authorization processing for the following Cardholder activities:

- Authorization Requests for Card transactions, including:
  - Visa Card-present and Card-not-present (mail order, telephone order, electronic commerce, Partial Authorization, recurring payment, instalment payment, or contactless) purchase transactions, and cash transactions (ATM, manual cash, and quasi-cash)
  - Visa Smart Debit/Credit (VSDC) transactions
  - MasterCard POS balance inquiry, Account Verification, and purchase transactions (in-person and mail order, telephone order, and electronic commerce), and cash transactions (manual cash and quasi-cash) for Banknet (MasterCard's transaction processing network)

  **Note** The Visa Europe System does not provide stand-in processing for MasterCard transactions.

  - American Express authorizations, Partial Authorizations, and balance returns
  - American Express, Diners Club International (DCI), and Discover International purchase transactions

  **Note** When the Visa Europe System receives Diners Club International authorization requests, it routes them to Diners Club through the Discover Gateway to the Discover Network. However, with the exception of having the same routing path, Diners Club and Discover International products are separate products and the Visa Europe System processes them each according to their separate requirements.

  - Private-label Card purchase transactions (in-person and mail order, telephone order, and electronic commerce)
  - Proprietary Card purchase transactions (in-person and mail order, telephone order, and electronic commerce), and cash transactions (ATM and manual cash)

  **Note** Private-label or Proprietary Card processing is subject to individual agreements between the Issuer and Visa Europe.

  - Address verification for Authorization Requests when the Acquirer requests verification and participates in the Address Verification Service (AVS)
- Reversals of previously approved transactions
- File updates and inquiries

### Transaction logging

Each VIC maintains a log of all requests and responses that the DMSA component processes.

The system records key information in the message, together with the outcome of conversions, validations and other in-flight processing performed by VEAS (such as CVV validation). When the transaction is complete, DMSA passes relevant information from the system log to the DMSA offline system components, which use the data for reporting, billing, and other administrative functions.

#### System management

DMSA also supports online network management and administrative messages that control user access for DMSA processing and provide system status information to Processing Centres for DMSA.

#### Overview of each DMSA online processing function

The following subsections describe the functions of DMSA online processing.

### 2.3.1 Initial message parsing and editing

When DMSA receives a message, it performs initial checks to ensure that the message is valid and is correctly formatted. DMSA checks the message type and ensures that the sender included all required fields for that message.

DMSA also performs functions, or services, as specified by the Member. These functions include:

- Message enhancement
- Currency conversion through the Multicurrency Service

For information about the Multicurrency Service, refer to the *Visa Europe Technical Service Descriptions*.

See Chapter 5, *Initial message parsing and editing*, for more information.

### 2.3.2 Message processing

DMSA also performs functions, or services, as specified by the Member. These functions include:

- Visa Security Module (VSM) functions, including Chip authentication, PIN translation
- Magnetic stripe or Chip-based CVV, Integrated Card Verification Value (iCVV), Card Verification Value 2 (CVV2), Card Authentication Verification Value (CAVV), and Dynamic Card Verification Value (dCVV) verification
- Custom Payment Service (CPS) reimbursement program screening

Refer to the *Visa Europe Technical Service Descriptions* for information about:

- The Card Verification Service, for validation of the magnetic stripe-based or Chip-based CVV and CVV2
- The PIN Verification Service, for PIN Verification methods
- The Verified by Visa Service, for validation of the CAVV
- CPS/ATM, refer to the description of Custom Payment Service/ATM

Currently, there are no CPS/POS programs running within the Visa Europe Territory. These programs may however be utilised by Processors running cross-border activities. For more information, please refer to the V.I.P. system manuals.

See Chapter 6, *Message processing*, for more information.

### 2.3.3 Message routing

Message routing is an important function of DMSA. Routing refers to sending messages between the Visa Europe System and Acquirers and Issuers. The term also applies to the decisions VEAS makes as to whether to route messages to Issuers or to STIP.

**Note** DMSA Acquirers must use Visa-supplied account range routing tables for ATM Transactions. DMSA Acquirers can use, at their option, Visa-supplied account range routing tables for POS transactions.

DMSA first looks at several factors such as the Account Number and the destination address when determining how to route a transaction.

DMSA also makes the decision to route an Authorization Request to the Issuer or to STIP for processing depending on the following parameters the Issuer selects for its processing:

- Processing limits for when the Issuer is available
- Positive Cardholder Authorization Service (PCAS) parameters

See Section 6.4, *Risk level and limits determination*, for more information about DMSA routing.

Members may also select additional routing services, such as the ATM/POS Split Routing Service (and its Alternate Routing option) and the PIN/No-PIN Split Routing Service, which affect DMSA routing decisions. For non-Visa transactions with destinations outside of the Visa Europe System network, Authorization Gateway Services determine routing. For further information, refer to the *Visa Europe Technical Service Descriptions*.

See Chapter 7, *Message routing*, for further information.

### 2.3.4 Stand-in processing

STIP occurs when VEAS acts as a back-up Processor and authorizes or declines transactions on the Issuer's behalf.

If the conditions of the Cardholder account and the transaction require that the Issuer, rather than STIP, should make the final authorization decision, DMSA uses Issuer-specified or Visa Europe-specified mandated minimum Issuer limits to forward the request message to available Issuers. If the Issuer is unavailable, STIP then processes the transaction according to Issuer-unavailable parameters.

The parameters that STIP uses to approve or decline a transaction include Issuer-specified activity limits, advice limits, and any Cardholder risk-level limits and random selection factors. Issuers can maintain files of Cardholder data at the VIC and can select the limits that control which transactions STIP can approve. Some other card programs processed according to Visa rules are also eligible for STIP at the Issuer's discretion.

See Chapter 8, *Stand-in processing (STIP)*, for detailed information about STIP and about establishing activity, advice, and Cardholder risk-level limits as well as random selection factors.

DMSA usually creates advices for Issuers to inform them of actions taken by STIP on their behalf, including performing stand-in authorizations, reversals, and Cardholder Database updates. Issuers may recover their advice data from the DMSA advice file at their VIC.

For a description of advice recovery through the DMSA Advice Retrieval Service, refer to the *Visa Europe Technical Service Descriptions*.

## 2.4 DMSA offline functions

After the online real-time processing of Cardholder transaction messages, DMSA transfers information pertaining to those messages from the system log to offline reporting and billing programs. DMSA offline functions include:

- Reporting (includes authorization reports, Exception File and Advice File reports, and POS reports) and generation of Card Recovery Bulletins for Visa Cards
- Managing DMSA tables and databases

For technical details about the DMSA offline functions, refer to the *DMSA Technical Specifications*.

### 2.4.1 Reporting

The DMSA reporting system generates various reports available to Members by subscription. These reports describe DMSA authorization activity and Cardholder listings in the exception and advice files. The system also produces POS and downgraded transaction reports for Acquirers. These reports provide individual transaction and summary information. Issuers and Acquirers can also subscribe to certain reports in raw data file format.

DMSA reporting systems generate the following sets of reports:

- Authorization Profile Reports (APRs)
- Cardholder Database reports, including the Advice File Listing Report, the Exception File reports, and data files
- POS reports
- CPS downgrade reports

For descriptions and samples of reports, refer to *SMS and DMSA Reports*.

### 2.4.2 Managing DMSA tables and databases

DMSA uses information supplied by Members to process Authorization Request messages. Once Members select options and establish limits and parameters such as those for Merchant Category Groups (MCGs), DMSA maintains records of routing and processing rules that apply to BINs, to Processing Centres, to stations. DMSA stores these parameters in the system tables.

Members add, change, and delete this information, as needed, to reflect business changes.

Depending on the services selected by the Member, DMSA can automatically update information in these DMSA databases at the time of the transaction.

VEAS also keeps records of the following relationships:

- Issuers to Account Numbers
- Issuers and Acquirers to Processing Centres
- Processing Centres to VICs
- Processing Centres to network stations

Members must report any changes in Account Numbers and account ranges or in Processing Centre designations to Visa Europe. This information is vital to the correct routing of messages.

### 2.4.3 Cardholder Database files

The Cardholder Database contains Account Numbers and other data that STIP uses to process address verifications, PIN Verifications and Account Verifications.

STIP also uses the database to store advices until Issuers retrieve them. The Cardholder Database comprises files maintained by Visa, by the Issuer, and by both. Members can update their files through online messages or by requesting updates through Visa Europe Customer Support, VROL or GCAS. Account managers either provide a list of BINs and Account Numbers, or BINs and field 41 - Card Acceptor Terminal Identification and field 42 - Card Acceptor Identification Code for the requests.

Table 1 lists the files contained in the Cardholder Database. Appendix A, *Cardholder Database and Advice Files*, describes the files in more detail.

**Table 1: Cardholder Database files**

| Cardholder Database files | |
|---|---|
| **File** | **Summary description** |
| Activity File | This Visa-generated file contains accumulated counts and amounts of Visa-approved transactions and can include accumulated totals of Issuer-approved transactions as well as the count of consecutive invalid PIN-entry attempts accumulated by STIP. |
| Advice File | This Visa-generated file contains STIP processing records that inform Issuers of STIP decisions made on their behalf for authorizations, verification-only requests, and reversals. |
| Exception File | Issuers create and maintain this file. It contains positive and negative action codes and other special instructions that indicate that the Cardholder's account requires special attention, for instance, the Merchant should pick up the Card at the point-of-service. VEAS also uses it to create Cardholder Recovery Bulletins (CRBs). |
| PIN Verification File | Issuers create and maintain this file and the optional PIN Verification Service uses it. The file contains Visa PIN Verification Values (PVVs) and PIN Verification Key Indexes (PVKIs) when the Issuer uses the Visa PVV method of PIN Verification. |
| Risk-Level File | Issuers create and maintain this file and VEAS uses it for assigning and maintaining individual Cardholder's risk levels, daily spending limits, and Merchant group daily activity limits. |

## 2.5 Authorization response codes

The Issuer, or STIP on behalf of the Issuer, provides a response code to each Authorization Request. The response code indicates whether or not the transaction has been authorized, and can indicate what action the Merchant should take, such as picking up the Card.

The response code is held in field 39, which is present in all responses except those for reconciliation and most network management functions. For more detailed information about field 39 and its valid values, refer to the *DMSA Technical Specifications*.

A single transaction might incur more than one response code, for example, an activity limit might be exceeded and a Card verification might fail. If STIP processes the transaction, it compares all response codes generated so far and selects the one with the highest priority (indicating the most risk or the greatest message error). It then updates the activity accumulators, sends an advice to the Issuer, and if necessary, converts the response code for the Merchant. For example, if the PIN-entry activity is exceeded, STIP forwards the response to the Issuer. The response code to the Acquirer/Merchant contains an approval or decline response code as specified by the Issuer in the system tables. In certain situations, STIP forward-refers a transaction to the Issuer. The Issuer then provides a response. For information about STIP processing and advice generation, see Chapter 8, *Stand-in processing (STIP)*.

# 3 DMSA participation requirements

Issuers can choose to have all of their transactions processed by DMSA and DMSC, by SMS, or by DMSA, DMSC, and SMS. Issuers also can choose to use different processing methods for different Visa products.

Members that choose DMSA processing must fulfil all of the DMSA participation requirements. These requirements can vary, depending on whether the Member is a DMSA Issuer or Acquirer and on which access devices and processing options the Member selects.

Members connecting to DMSA must consider:

- Visa Europe System access devices
- Processing options and parameters
- Message support requirements
- Resolving transaction failures

The following sections identify basic system requirements, options, and parameters for Acquirers and for Issuers. Members can contact Visa Europe Customer Support for complete requirements, available options, and help in establishing parameters.

## 3.1 Visa Europe System access devices

Acquirers and Issuers determine optimal access device options by considering their respective transaction volume, physical location in the world, and the types of services they support for their Merchants. For instance, a DMSA and SMS Processing Centre may use a single EA Server for both DMSA and SMS messages, or it may use a separate EA Server for DMSA and SMS.

The choice depends on the centre's system configuration; separate host computers for DMSA and for SMS processing require logically separate processing endpoints to keep DMSA and SMS traffic separate

**Important** A single host may be configured with one or with two Visa Europe System access devices

Interface requirements depend on the type of device selected, although currently the only option is the EA Server.

## 3.2 DMSA processing options and parameters

DMSA offers several processing options for maximum flexibility. Members and system users control DMSA processing primarily by selecting options and then establishing parameters (also called limits). DMSA executes the majority of system functions according to these user-selected parameters, which VEAS stores in the system tables.

Members connected to DMSA must select the processing options best suited to them and to the types of transaction traffic they support. Services and processing options include those applicable at the BIN level, at the Processing Centre level, and at the individual Processing Centre station level.

## 3.3 Acquirer considerations

Acquirers must determine their policies for processing DMSA transactions. Issuers must establish parameters for message response times and must determine the actions that DMSA is to take when they fail to respond within the prescribed time. Adequate time must be allowed for Issuer centres to respond, but Issuers, in turn, must be responsive to the time-out demands of their electronic terminals and ATMs. To be certified by Visa Europe, they must support timed-out transactions.

### 3.3.1 Timed-out transactions

If an Acquirer experiences a time-out, it must do one of the following:

- Retry the transaction

  The Acquirer must send a reversal of the original request or a repeat of the original request. Visa Europe recommends sending both a reversal and a repeat.

- Reverse the transaction

  The Acquirer decides not to retry the transaction; it must send a reversal of the original request.

  **Note** Because the Acquirer did not receive a response from VEAS, the Acquirer does not know whether the transaction was approved or declined. Accordingly, the Acquirer can request a reversal with field 38 - Authorization Identification Response containing all zeroes or all blanks. If field 38 is not present, VEAS rejects the reversal request with reject code 0293 (field 38 missing).

See Section 4.4.3, *How VEAS processes repeat (duplicate) Authorization Requests*, for further information about timed-out messages.

### 3.3.2 Submitting Authorization Requests in batches

To prevent volume spikes from overloading Issuers' processing systems, Acquirers must not submit Authorization Requests in batches ordered by Account Number or by BIN.

## 3.4 Issuer considerations

Issuers must establish in-house Processing Centres or must designate other Processing Centres or third-party Processors to perform the necessary Issuer and Cardholder functions.

Issuers must also establish parameters (limits) for DMSA to use when it makes routing and STIP authorization decisions. There are three main types of limits: Issuer limits, advice limits, and activity limits. See Section 6.4, *Risk level and limits determination* and to Chapter 8, *Stand-in processing (STIP)*, for detailed information about these and other parameters. VEAS stores the limits in the system tables and in the Cardholder Database. See Appendix A, *Cardholder Database and Advice Files*, for information about this database.

## 3.5 Message support requirements for Acquirers and Issuers

Issuers and Acquirers must fulfil all DMSA message support requirements. Message support includes the following:

- The logic necessary to generate the right type of request message for the function desired and to process the response appropriately
- Files, logic, or both, as needed, to supply data required in the DMSA request when it is not available from the point of sale or point-of-service
- The ability to manage all of the messages related to any given Cardholder transaction set

  Members must avoid duplicate postings and must accurately calculate settlement totals
- Support for any optional system feature or service used by the Member

  Examples include the Address Verification Service (AVS), the PIN Verification Service (PVS), and the Real Time Scoring Service (RTS). For information about services provided by Visa Europe, refer to the publications listed in Section 1.6, *Related information.*
- Downtime procedures and appropriate recovery

Members can contact Visa Europe Customer Support for complete information about full support requirements for DMSA messages.

### 3.5.1 Message formats

Visa Europe requires that DMSA Processors use the V.I.P. message format, which facilitates message processing between DMSA and SMS Members.

See Chapter 4, *DMSA messages and flows*, for further descriptions of these message formats.

For more detailed information about the V.I.P message format, refer to the *Introducing SMS and DMSA Messages*.

### 3.5.2 Certification

Visa Europe must certify that Member centres can process messages before they can use VEAS. Members can contact Visa Europe Customer Support for complete information about testing and certification.

### 3.5.3 Additional message processing procedures for Acquirers

DMSA Acquirers must ensure that their card processing systems are capable of generating and of receiving all of the various Visa Europe System messages necessary for the types of card processing the centres support. To accomplish this, they must:

- Convert the Issuer response to an adequate description for a terminal display at the POS device that does not change the meaning of the Issuer's response

  For example, Acquirers must convey a Card pick-up request to a Merchant explicitly, not as a simple decline.
- Establish procedures to handle non-routine responses from the Issuer, such as DMSA referrals or partial approvals, as applicable
- Support reversal messages. DMSA centres use reversals to cancel previously approved transactions

SMS Acquirers should consider how they might want to integrate various exception items into their authorization and clearing systems. They must:

- Establish policies and procedures for processing Chargebacks and representments, as well as for handling adjustments (for merchandise returns, failures at ATMs, and other back office corrections)
- Establish procedures that comply with the requirements for processing requests for originals and copies of sales drafts

### 3.5.4 Acquirer reversal processing

Before generating authorization reversal requests, Acquirers must wait for authorization approval responses. This precaution ensures that the authorization reversal request contains the appropriate fields from the original Authorization Request, such as field 38 - Authorization Identification Response.

**Note** Field 38 is mandatory only in authorization reversals, but not in 0420 financial reversals. An SMS Acquirer may submit a reversal of a financial transaction before it receives the response to the original and in that situation, the reversal would not contain field 38.

For timed-out Authorization Requests, Acquirers may populate field 38 with all spaces/zeroes. Because the Acquirer did not receive an Authorization Response from VEAS, the Acquirer does not know whether the Authorization Request was approved or declined. Accordingly, the Acquirer can request an authorization reversal with field 38 containing all spaces/zeroes because VEAS rejects the authorization reversal request if field 38 is not present with reject code 293 - (field 38 missing).

See Section 4.4.3, *How VEAS processes repeat (duplicate) Authorization Requests,* for further information about timed-out messages.

### 3.5.5 Processing rules for field 95 in ATM reversals

If an Acquirer submits an ATM partial reversal with an amount in field 95 – Replacement Amounts greater than or less than the amount in field 4 - Amount, Transaction and not zeros, Visa Europe processes the partial reversal transaction.

However, Visa Europe rejects the transaction with reject code 0115 (invalid value) if:

- An Acquirer submits a partial reversal with the amount in field 95 equal to the amount in field 4
- An Acquirer submits a partial reversal with an amount of zeros in field 95
- An Acquirer submits a full reversal with field 95 in the message

### 3.5.6 Processing of multiple partial reversals

DMSA does not retain message data from previous reversals. DMSA processes multiple partial reversals as long as the amount in field 95 - Replacement Amounts is less than the amount in field 4 - Amount, Transaction in each transaction. STIP does not update activity totals when processing reversals. See Section 8.13.1.1, *Activity testing on reversals*, for more information about reversal processing and about activity checking.

### 3.5.7 Issuer reversal processing

When Issuers receive a reversal request, they must return an acknowledgment response message to the Acquirer and must try to adjust the Cardholder's available balance. Depending on the message content, the acknowledgment response advises the Acquirer that the reversal is valid, or that the Issuer has a problem.

**Note** DMSA does not maintain transaction histories after the Visa Europe System or the Issuer sends a response. Therefore, DMSA cannot match reversals to originals, and cannot always approve reversals processed by STIP.

If the Issuer can match the reversal with a prior authorization and can adjust Cardholder records accordingly, the reversal response must contain the following amount information:

- For full reversal responses, the message must contain the amount from the reversal request.
- For partial reversal responses, the message must contain the original Transaction Amount and the replacement amount.

If the Issuer cannot match a reversal request to an original transaction, it must use the appropriate response code and must place a zero amount in the response message.

This coding indicates one of the following problems:

- The Account Number is incorrect
- The value of a full reversal request is incorrect
- The Issuer cannot reconcile the value of a partial reversal with the original Transaction Amount
- The reversal is possibly correct, but the Issuer cannot match it with the original because STIP processed the original (the Issuer may not be aware that STIP processed the original transaction)

**Note** The Visa Europe System does not allow zero amounts in reversal requests from Acquirers.

## 3.6 Resolving transaction failures

Occasionally, Member-initiated transactions fail to process as anticipated; for instance, VEAS might reject a request because of an invalid field value.

Members can research transaction failures by using tools such as the Visa Transaction Research Service (VTRS) or the transaction inquiry facility in Visa Resolve Online (VROL). Visa Europe Member representatives can also help resolve such problems.

### 3.6.1 The role of Visa Europe Member representatives

It is important that the Member gathers as much detailed information as possible about the transaction and the events surrounding it. The Member should collect the following information (when feasible) before contacting support:

- The time and date in Greenwich Mean Time (GMT), of the occurrence, as accurately as possible
- Transaction details, for example, Retrieval Reference Number, Account Number (securely encrypted), System Trace Audit Number and the BIN

- The circumstances surrounding the issue, for example, did the Member recently perform an upgrade, or did the incident occur after a certain time and date indicating a possible trigger
- Any possible patterns, for example, the incident occurs with every transaction, only occurs at certain times of day, or only occurs from a specific BIN
- The impact, the Visa brand, the number of transactions up to this point, the number of transactions per hour, and the Transaction Amounts affected

The support teams can start analysing the situation immediately instead of spending time gathering the information first.

To resolve these events as quickly as possible, Visa Europe Customer Support should be contacted.

# 4 DMSA messages and flows

This chapter describes DMSA message formats, structure, types, and sets. It also explains how various types of DMSA messages flow among Issuers, Acquirers, and VEAS.

**Important** Visa Europe strongly urges Members and their Processors to comply with mandatory field requirements.

In the VEAS documentation suite, the term mandatory refers to a Member requirement and means that a field must be present in a message and must contain certain values. Conditional refers to a Member requirement that applies under specified conditions. While VEAS enforces edits and rejects transactions for some violations of mandatory requirements, VEAS does not enforce edits for all mandatory or conditional fields and values.

Failure to do so can result in greater risk to the Member or increased processing costs, and may result in exposure to Chargebacks and Compliance claims, elevated decline rates, and disqualification for preferential Interchange rates. Visa Europe also advises Members not to rely on VEAS to reject all transactions that do not comply with mandatory or conditional requirements.

## 4.1 Messages

Two primary functions of DMSA are message management and message routing. To ensure that the Visa Europe System processes and routes messages correctly, Visa has set standards for how Acquirers and Issuers are to format messages.

DMSA edits request messages from an Acquirer for valid content and syntax before routing them to the Issuer or to stand-in processing (STIP) for authorization. DMSA also edits the response messages returned by the Issuer.

Both DMSA and SMS support V.I.P. message format. This enables Members and Processors to use either processing system for their transactions as they prefer. The V.I.P. message format has a maximum length of 800 bytes.

### 4.1.1 BASE I and V.I.P. alignment - Background

BASE I was the original name for Visa's authorization processing system; and SMS the name of its full financial processing system. The format of messages on those respective systems was originally defined as BASE I message format and V.I.P. message format respectively.

For a number of years, BASE I users were able to use either BASE I message format or V.I.P. message format. SMS users were only able to use V.I.P. message format.

Visa Inc. has since aligned authorization processing and single message processing in preparation for moving all of authorization processing onto one platform. The existing SMS was selected as a basis for all future development, and BASE I users will be migrated to that system.

In preparation for the migration of Processors from the BASE I system:

- SMS was renamed as V.I.P. System
- The V.I.P. System defines a new type of endpoint: Authorization Only (no full-financial message processing)
- The BASE I system was enhanced to behave more like the V.I.P. System
- The V.I.P. System was enhanced to provide more BASE I system functions, for example, PCAS
- Authorization message content and message edits were made the same on both the BASE I system and V.I.P. System (that is, the differences between the BASE I and V.I.P. message formats were virtually eliminated)

### 4.1.2 VEAS: V.I.P. message format processing

Since Visa Europe introduced its own VEAS system in 2006, which supports both DMSA and SMS message processing, it has been making changes in parallel with V.I.P. to ensure that interoperability is maintained. Processors within Visa Europe are therefore keeping aligned with authorization Processors in the rest of the world.

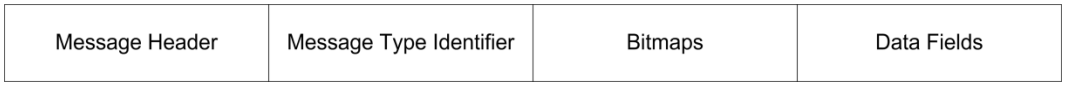
As the BASE I message format is now the equivalent of the V.I.P. message format, VEAS documentation assumes all Processors are utilising the V.I.P. message format. BASE I message format is no longer documented.

### 4.1.3 Message structure

Visa bases its authorization message formats and content on ISO standards, documented in *International Organization for Standardization (ISO) 8583; 1987 (E): Bank Card Organizational Messages - Interchange Message Specifications - Content for Financial Transactions*. To assist in message routing, authorization messages are prefaced with a message header and message type identifier. Subsequently each message contains one or more bitmaps, which are fields that indicate the content of the fields that follow, so that messages only transmit appropriate and necessary data, with no extraneous or unnecessary data.

Figure 6 illustrates the message elements that each bitmapped message contains.

**Figure 6: DMSA message structure**




These elements have the following characteristics:

- **Message Header**: The message's first element contains basic message identifiers and routing information along with message processing control codes and flags.
- **Message Type Identifier**: This second element contains a 4-digit code that specifies the message class and the category of function. For instance, 0100 indicates an Authorization Request. All messages contain a message type identifier.

- **Bitmaps** (one or more): This third element specifies which fields are present in a message. In addition to a primary bitmap, messages can include second and third bitmaps. Each map contains 64-bit fields, corresponding to the number of possible fields in a message.

  Map 1 = Fields 2-64

  Map 2 = Fields 65-128

  Map 3 = Fields 129-191

  - If a field is present in the message, the initiator sets the corresponding bit to 1; if that field is absent, the initiator sets its bit to 0. For instance, if the message contains field 44, the initiator sets bit 44 to 1. If field 44 is not in the message, the initiator sets bit 44 to 0.
  - If bit 1 of the first bitmap is 1, the message contains a second bitmap. Bitmaps 2 and 3 are present only when the message contains one or more of fields 65-128 and 129-191, respectively.
- **Fields**: A variable number of fields comprise the fourth element of a message and contain the information needed for processing a message related to a Cardholder transaction or for performing another system function. Established specifications uniquely define attributes, such as length and format, for each field.
  - Field content and length may be fixed or variable, depending on the type of message.
  - Many of the fields are fixed-length; however, where appropriate, fields are variable-length to eliminate transmission of unnecessary fill characters. Some fields may also be in the ISO tag-length-value (TLV) format. The TLV format contains a tag, a binary element that identifies the information that is to follow, a length element that defines the length of the field, and the value element that contains the information being conveyed.
  - To further save transmission costs throughout the system, Visa Europe System users format almost every numeric field in packed format, which cuts the field length in half.

For detailed information about the message header, bitmaps, and fields, refer to *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Messages* and the *DMSA Technical Specifications*.

### 4.1.4 DMSA message types

DMSA processes two basic categories of messages:

- **Authorization-related messages**: Authorization-related messages include all messages from Acquirers that request authorization of a transaction, including voice-based Authorization Requests, as well as messages from Issuers or from STIP that respond to Authorization Requests with approval or decline decisions. They also include other authorization messages such as verification requests and ATM balance inquiries.

  Telephone-based voice Authorization Requests occur in situations in which a Merchant calls its Acquirer and reads the Account Number over the telephone as Acquirer staff enters it at a terminal. Voice authorizations also include transactions for which staff enters Card information directly into a computer through a series of digitised voice

prompts (for instance, through VoiceTec software). The terminal then generates the 0100 Authorization Request.

**Note** The VEAS documentation manuals also use the term **voice** in the context of approving an Authorization Request. This usage is in keeping with the term's usage in the *Visa Europe Operating Regulations*, which describes voice authorizations as a method of responding to Authorization Requests.

- **Non-Authorization-Related Messages**: Non-authorization-related messages include various administrative, file update, and system management messages not directly related to the authorization of transactions.

As stated in Section 4.1.3, *Message structure*, each message type has an identifier associated with it, such as 0100 that helps identify what type of message it is. However, entities can use an identifier for more than one type of message. For instance, Members use 0100 messages to request authorization or Cash Disbursement processing for several Card products.

Table 2 lists DMSA authorization-related message type identifiers and their associated message types.

**Table 2: DMSA authorization-related message types**

| DMSA authorization-related message types | |
|---|---|
| **Message identifier** | **Message type** |
| **Cardholder Transactions** | |
| 0100 | ATM or POS Balance Inquiry<br>Authorization Request<br>Authorization Status Check Request<br>Incremental Authorization Request<br>Prepaid Activation Request<br>Prepaid Activation and Load Request<br>Prepaid Load Request<br>Prepaid Partial Load Request<br>Recurring Payment Request |
| 0110 | Authorization Response<br>Authorization Status Check Response<br>Balance Inquiry Response<br>Incremental Authorization Response<br>Partial Approval Response<br>Prepaid Activation Response<br>Prepaid Activation and Load Response<br>Prepaid Activation and Partial Load Response<br>Prepaid Load Response<br>Prepaid Partial Load Response<br>Recurring Payment Response |
| 0120 | AFD confirmation advice |
| 0130 | Advice Receipt Acknowledgement (optional) |

| DMSA authorization-related message types | |
|---|---|
| **Message identifier** | **Message type** |
| 0400 | Reversal Notification<br>Reversal - Partial Approval<br>Reversal - Void of Activation<br>Reversal - Void of Load |
| 0410 | Reversal Response<br>Reversal - Partial Approval Response<br>Reversal - Void of Activation Response<br>Reversal - Void of Load Response |
| 0420 | ATM – Adjustment (optional) |
| 0430 | ATM – Adjustment Response |
| **System-Generated Transactions** | |
| 0120 | Authorization Advice<br>Balance Inquiry Advice<br>File Update Advice<br>Discrepancy Advice |
| 0420 | Reversal Advice |
| 0130 | Advice Receipt Acknowledgement (optional) |
| 0430 | Advice Receipt Acknowledgement (optional) |

Table 3 lists all DMSA non-authorization-related message identifiers and their associated message types.

**Table 3: DMSA non-authorization-related message types**

| DMSA non-authorization-related message types | |
|---|---|
| **Message identifier** | **Message type** |
| **File Update Transactions** | |
| 0302 | File Update or Inquiry Request (Issuer) |
| 0312 | File Update or Inquiry Response (Issuer) |
| 0322 | File Update or Discrepancy Advice |
| 0332 | File Advice Receipt Acknowledgement |
| **Administrative transactions** | |
| 0600 | Administrative Request |
| 0610 | Administrative Response |
| 0800 | Network Management Request |
| 0810 | Network Management Response |

Visa Card transactions can consist of all of the DMSA message types shown in Table 2 and Table 3. The Visa Europe System limits other Card transactions to the message types listed in Table 4.

**Table 4: Card types and their allowable DMSA message types**

| Card types and their allowable DMSA message types | | |
|---|---|---|
| **Card type** | **Message type** | **Comments** |
| Plus | 0100 Authorization Request<br>0110 Authorization Response<br>0100 ATM Balance Inquiry<br>0110 ATM Balance Inquiry Response<br>0120 Authorization Advice<br>0400 Reversal Request<br>0410 Reversal Response<br>0420 Reversal Advice | n/a |
| Visa Member Proprietary | 0100 Authorization Request<br>0110 Authorization Response<br>0120 Authorization Advice<br>0400 Reversal Request<br>0410 Reversal Response<br>0420 Reversal Advice | For instance: Bank ATM Card |
| Private Label | 0100 Authorization Request<br>0110 Authorization Response<br>0120 Authorization Advice<br>0400 Reversal Request<br>0410 Reversal Response<br>0420 Reversal Advice | For instance: Discover card, JCB card, department store credit card |
| MasterCard | 0100 Authorization Request<br>0110 Authorization Response<br>0100 Balance Inquiry Request<br>0110 Balance Inquiry Response<br>0400 Reversal Request<br>0410 Reversal Response | Includes Banknet |
| Travel & Entertainment (T&E) | 0100 Authorization Request<br>0110 Authorization Response | US region T&E Cards include American Express, Carte Blanche, Diners Club |
| Amadeus/SITA Airline Networks | 0100 Authorization Request<br>0110 Authorization Response | **Note** Amadeus/SITA transactions enable Airline ticket agents to authorize Visa transactions without having to first call an Acquirer. |

### 4.1.5 Message sets

A message set consists of the allowable messages that can be used as part of a given Cardholder transaction. Use of message sets provides the Acquirer, the Issuer, and VEAS with the means to link messages and to control real-time account posting and settlement accumulator updating. A Cardholder transaction is comprised of a variable number of messages contained in its message set.

Table 5 lists the DMSA Cardholder transactions and their associated message sets.

**Table 5: DMSA Cardholder transactions and their message sets**

| DMSA Cardholder transactions and their message sets | | |
|---|---|---|
| **Cardholder transactions** | **Message set** | **Comments** |
| Authorization or Confirmation for POS, ATM, Visa Smart Debit/Credit (VSDC), Electronic Commerce, and Contactless | 0100 Request<br>0110 Response<br>0120 Advice<br>0400 Reversal<br>0410 Response<br>0420 Advice | Acquirers must send confirmation to Issuers for a misdispense of an International Transaction using a Card at an ATM or Plus ATM.<br>**Note** A misdispense occurs when the amount of the funds that a Cardholder actually receives differs from the requested amount. |
| POS Account Number, Address, or Card Verification Value (CVV) Verification using a USD 0 Transaction Amount | 0100 Request<br>0110 Response<br>0120 Advice | **Note** Acquirers cannot reverse verifications. |
| ATM or POS Balance Inquiry | 0100 Request<br>0110 Response<br>0120 Advice | VSDC inquiries include Chip Card authentication. Acquirers cannot reverse balance inquiries. POS balance inquiries can be standalone or can be part of an Authorization Request. |

For a Cardholder transaction, Processors must use only the allowed messages in the associated message set. DMSA enforces these rules by comparing an incoming message with previous messages containing the same key data elements.

## 4.2 Message flows - Authorization-related

This section describes the DMSA message flows for various transactions. It also provides message flow diagrams to illustrate the processing that DMSA performs for each transaction type submitted using magnetic stripe- or Chip-based Cards and for Card-not-present (CNP) transactions.

Cardholders initiate Authorization Requests at a point of sale or point-of-service or at an ATM or Cash Disbursement approval from the Issuer of the Card. Merchants and Acquirers also use these requests for balance inquiries; Account Verifications and address verification requests.

**Note** Visa Europe Authorization Services can send 0100 Account Verification messages that contain Verified by Visa authentication data. VEAS authenticates the CAVV and performs standard Verified by Visa processing on these messages before forwarding them to Issuers.

### 4.2.1 Authorization Request (0100) and Authorization Response (0110) message flows

When DMSA receives an Authorization Request, it determines whether to forward it to the Issuer or to STIP, based on routing parameters. See Section 6.4, *Risk level and limits determination*, for information about establishing these parameters.

Figure 7 shows the typical Authorization Request message flow for an Authorization Request for a Visa, proprietary, or private-label Card transaction when the Visa Europe System sends the transaction to the Issuer and the Issuer is available. Issuers usually check a Cardholder's account balance or other amount records to determine if sufficient funds are available to approve a request. An approval indicates the Issuer's agreement to accept the transaction, provided that the Acquirer and the Visa Europe System follow all of the transaction's processing rules.

**Note** DMSA Issuers can choose to receive Authorization Request messages with time limits in field 63.2 - Time (Preauth Time Limit). Such authorizations are initiated by SMS Acquirers when the final Transaction Amount is not known (for example, Automated Fuel Dispenser (AFD) transactions). The time limit notifies the Issuer the time by when the Merchant or Acquirer intends to complete the transaction. Issuers choosing to receive field 63.2 must send the field in response messages.

**Figure 7: Authorization Request message flow - DMSA**

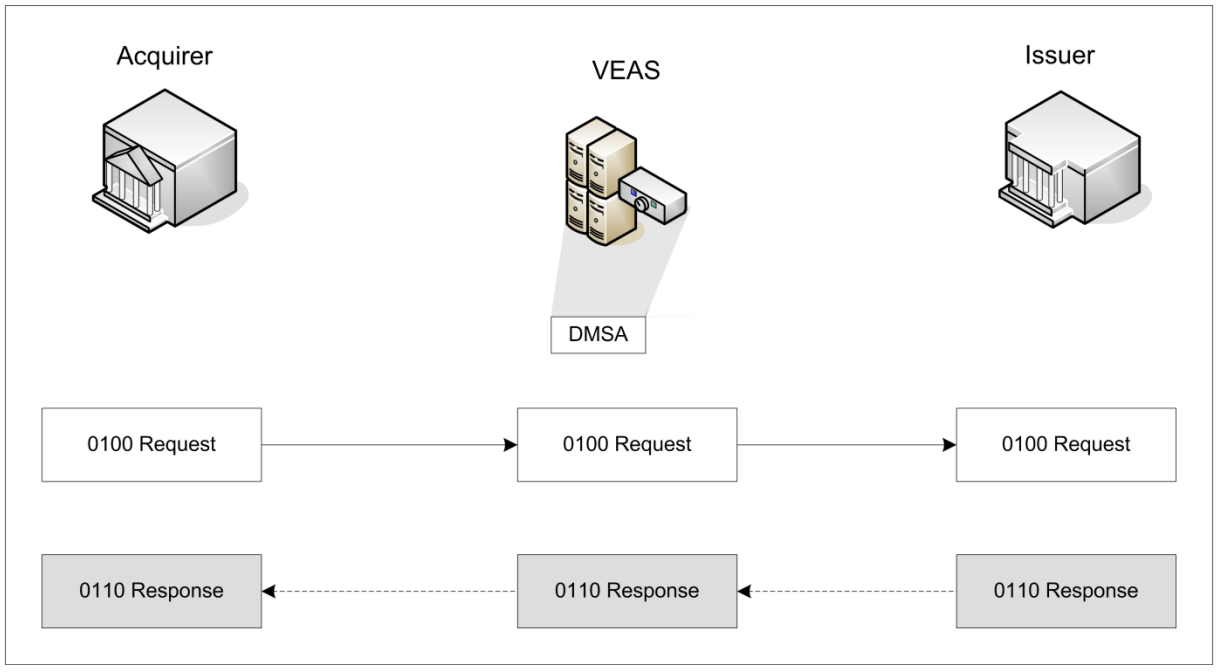
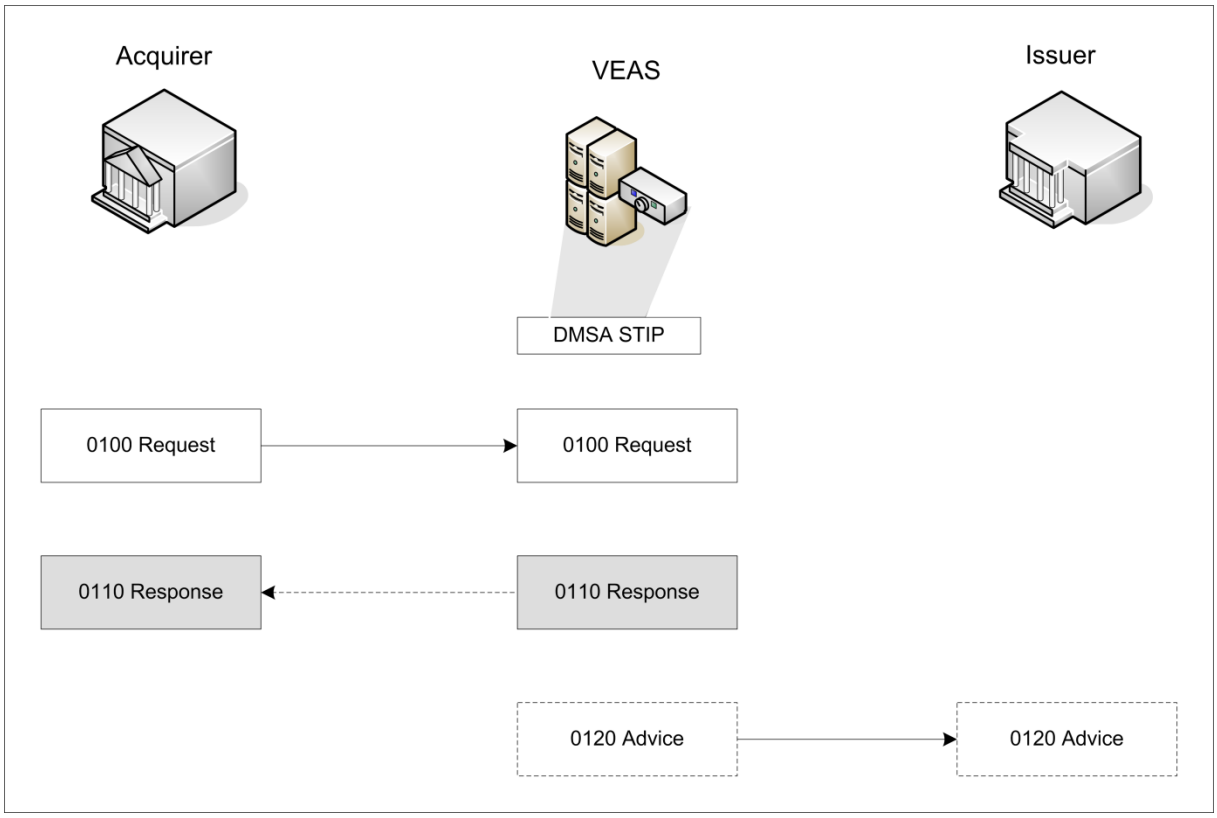



Figure 8 illustrates the message flow when STIP processes the transaction. In this case, DMSA STIP responds on behalf of the Issuer and creates an 0120 advice for the transaction.

If the Issuer is unavailable or VEAS is inoperative (STIP is not applicable or available for this transaction), the 0120 advice may contain response code 91 in field 39. For information about STIP processing and advice generation, see Chapter 8, *Stand-in processing (STIP)*.

**Figure 8: Authorization Request message flow - DMSA STIP**



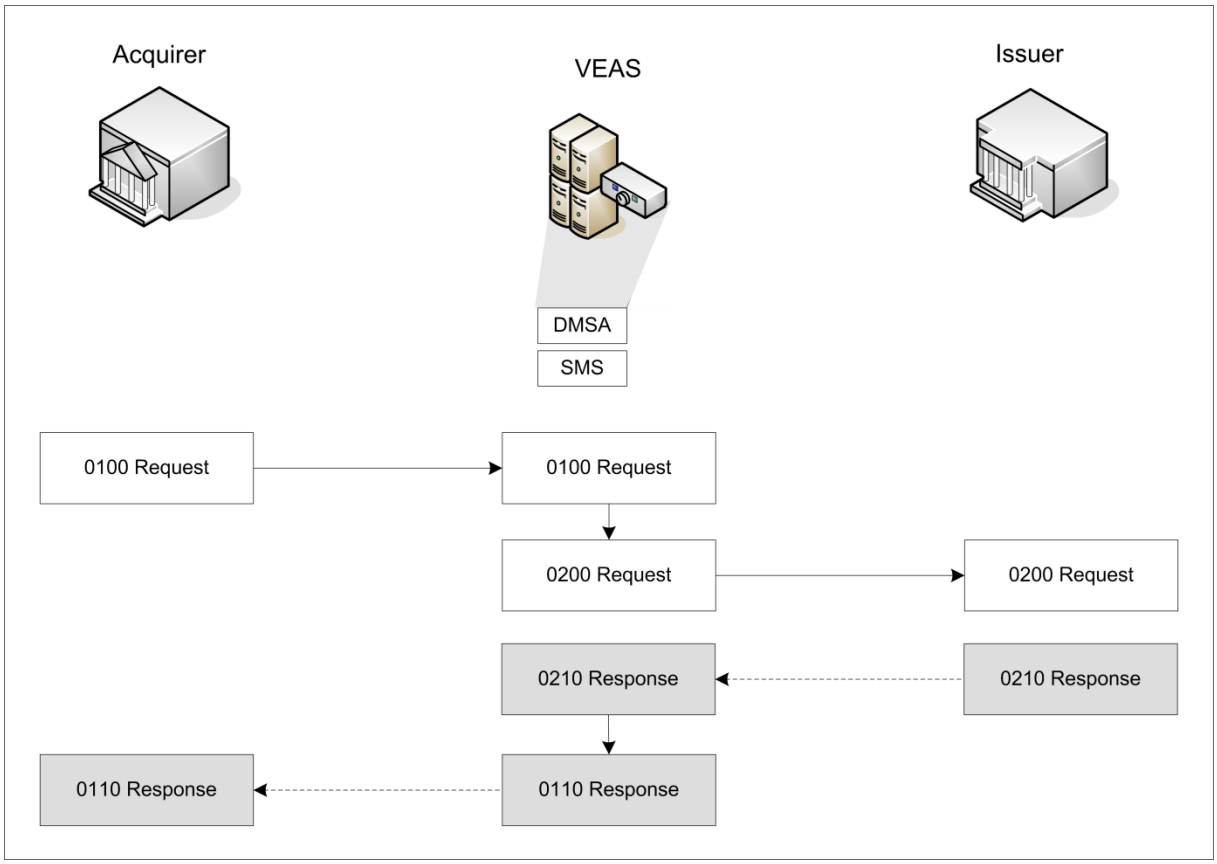

DMSA forwards responses from Issuers to Acquirers. When DMSA is unable to return a response (for instance, if the Acquirer Processor is down), DMSA logs and discards the response. The Acquirer then resends the Authorization Request.

### 4.2.2 Transactions between DMSA Acquirers and SMS Issuers

VEAS converts ATM 0100 Authorization Requests to SMS 0200 full financial requests when the Issuer participates in the ATM Format Conversion Service. The SMS Issuer sends an 0210 response back to VEAS, which converts it to an 0110 message and forwards the response to the DMSA Acquirer. VEAS does not convert 0100 POS Authorization Requests; it forwards them as is to SMS. SMS STIP performs any stand-in processing for SMS messages.

Figure 9 illustrates a typical Authorization Request message flow between a DMSA Acquirer and an SMS Issuer when the Issuer participates in the ATM Format Conversion Service.

**Figure 9: ATM Authorization Request message flow between a DMSA Acquirer and an SMS Issuer that participates in the ATM Format Conversion Service**




### 4.2.3 Balance inquiries

The Visa Europe System supports international ATM balance inquiries.

The Visa Europe System evaluates Processor-level parameters rather than BIN-level parameters to determine when Visa Europe sends balance information to Acquirer Processors in field 54.

For Acquirer Processors that receive balance information, Visa Europe no longer suppress the return of the balance information for specific BINs. The Acquirer Processor must manage the delivery of balance information to the Acquirer, ATM, or Merchant.

### 4.2.4 Balance inquiries at ATM

Acquirers are able to request the balance of a Cardholder's checking, savings, Credit Card, or other account using an ATM or POS request. For checking, savings, and accounts other than Credit Card accounts, Issuers either return the account-ledger balance or return the account-available balance. For Credit Card accounts, Issuers return either the amount of credit remaining to the Cardholder or return the Cardholder's credit limit.

The Issuer can be from any region. However, if the Issuer does not support balance inquiries, STIP returns a response indicating that the Issuer does not support the transaction.

When submitting a balance inquiry, SMS Acquirers use 0200 financial transactions containing processing code 30 - (available funds inquiry in positions 1-2). VEAS converts the 0200 message to an 0100 message and forwards it to the Processing Centre of the Issuer.

**Note** The Visa Europe System does not allow field 4 - Amount, Transaction in balance inquiries. If the field is present, VEAS rejects the message. The Visa Europe System does not include field 6 - Amount, Cardholder Billing, field 10 - Conversion Rate, Cardholder Billing, and field 51 - Currency Code, Cardholder Billing, in 0120 balance inquiry advices.

Issuers can receive balance inquiries for the following customer account types:

- Unspecified accounts
- Savings accounts
- Checking accounts
- Credit Card accounts
- Universal accounts (represented by customer identification numbers)

When the Issuer receives a balance inquiry, it returns the balance amount in field 54 - Additional Amounts of the response message. The Issuer also provides the currency code, indicates whether the balance is the account-ledger or account-available balance, and identifies if the balance is positive or negative. For Credit Card balances, the account-ledger balance is the amount of credit remaining to the Cardholder, and the account-available balance is the Cardholder's credit limit.

Issuers can also use field 54 to provide the account balance in its response to a cash withdrawal request.

When the Issuer is unavailable, STIP performs limited processing for these transactions because the account balance is not available. This processing consists of:

- Editing the Account Number
- Checking the Exception File in the Cardholder Database for a decline or pick-up code
- Creating an advice for the Issuer when a negative code is present in the Exception File

### 4.2.5 Balance inquiries at POS

Acquirers can submit supporting POS balance inquiries as standalone transactions or as part of Authorization Requests. POS balance inquiries are valid for the same customer account types as ATM balance inquiries and generally follow the same processing rules. However, DMSA POS balance inquiries do not require a PIN.

Participating Issuers can optionally return positive or negative balance information in field 54 in responses to standalone or purchase requests. Participating Merchants print balance data on the Cardholder's receipt. VEAS drops field 54 in responses if the Issuer's return response code indicates a lost or stolen Card, for instance, response code 43 (pick up Card, stolen Card). VEAS also drops field 54 in POS balance inquiry responses if their destination is an Acquirer that does not support POS balance services.

STIP is not available for standalone POS balance inquiries. VEAS declines transactions with response code 57 (transaction not permitted to Cardholder) in field 39 - Response Code. If the Issuer is unavailable for a standalone POS balance inquiry, VEAS declines the transaction with response code 91 (Issuer unavailable) to the Acquirer.

**Note** The Visa Europe System does not allow field 4 in balance inquiries. If the field is present, VEAS rejects the message. The Visa Europe System does not include field 6, field 10, and field 51 in 0120 balance inquiry advices.

STIP is available for balance inquiries with purchase Authorization Requests and uses Issuer-provided parameters for Issuer-unavailable conditions as if a balance inquiry were not involved. For further information, refer to the *DMSA Technical Specifications*.

### 4.2.6 MasterCard Authorization Requests

The Visa Europe System routes MasterCard Authorization Requests to Banknet. The Visa Europe System sends only non-PIN-based MasterCard requests to Banknet. DMSA declines attempts to submit PIN-based requests to Banknet with response code 91 (cryptographic error found) in field 39.

DMSA automatically converts messages from V.I.P. message format to the MasterCard format during message routing. The Visa Europe System converts V.I.P. message format requests received from Acquirers to the MasterCard format and routes them to the MasterCard Banknet network. Banknet returns the responses, and the Visa Europe System automatically reconverts the messages to V.I.P. message format and forwards the responses to the Acquirers.

Acquirers processing MasterCard transactions through the Visa Europe System must support field 42 - Card Acceptor Identification Code for 0100 and 0110 Authorization Requests and responses, and for 0400 and 0410 reversal messages. MasterCard Authorization Requests submitted with a value of 00 (goods or service purchase POS transaction only) in field 3 - Processing Code must include field 42 in the message. If the value in field 3 is 00 and field 42 is missing, VEAS inserts response code 96 (system malfunction or certain field error conditions) in field 39 in the response message.

All Acquirers supporting MasterCard transactions must also support field 38 - Authorization Identification Response, position 6 - MasterCard Values. When a request is approved, field 38 contains the account category value for the transaction in 0110 Authorization Responses. In case of a reversal, the values in the 0110 Authorization Response and in the reversal must match.

Acquirers must send field 62.17 - Gateway Transaction Identifier (Bit Map Format) in 0400 MasterCard reversal messages.

If an Acquirer sends field 104 - Transaction-Specific Data in a MasterCard 0100 authorization message, the field is also included in the Authorization Response message; reversal messages must also contain this field.

**Important** Acquirers must begin supporting field 104, Usage 2, by April 2012. Testing and activation by Visa Europe is required for a first-time implementation of field 104, Usage 2.

The Authorization Gateway to Banknet handles such MasterCard services as Card Verification Code 2 (CVC2), MasterCard's version of Card Verification Value 2 (CVV2). For more information, refer to the *DMSA Technical Specifications*.

**Note** Acquirers that process MasterCard transactions through VisaNet in the US region must support the financial network codes defined for field 62.17. Refer to *SMS POS Technical Specifications*, for network codes and requirements.

For details about data field mapping between Visa and MasterCard, refer to the *Authorization Gateway Service Cross-Reference Guide*.

### 4.2.7 Discover Authorization Requests

The Visa Europe System authorizes Discover transactions and routes them through the Discover Gateway for processing. The messages do not require formatting because Discover transactions use the V.I.P. message format.

The Visa Europe System delivers the request to the issuer's authorization centre for approval and returns a response to the Member or to the Merchant by the reverse path. If the Discover issuer is unavailable, DMSA STIP can check Card pick-up lists and Cardholder activity, and can generate responses and advices based on the results of the checks.

VEAS adds field 116 - Card Issuer Reference Data to 0110 Approval Responses that are generated by Discover. However, VEAS does not add this field to STIP approvals or messages containing non-Approval Response codes.

VEAS passes Dataset ID 68 in field 116 - Card Issuer Reference Data to Acquirers in 0110 responses, if it receives this dataset from the issuer.

Acquirers can include the ID Discover assigns in field 32 - Acquiring Institution Identification Code in authorization messages destined for Discover. In such cases, VEAS includes the ID in the 0110 response message it returns to Acquirers.

VEAS overlays any Acquirer-provided value in field 33 - Forwarding Institution Identification Code in request messages using a default value assigned by Discover. Field 33 is not returned to Acquirers in 0110, 0410 and 0430 responses.

For 0400 requests, VEAS overlays any Acquirer-provided value in positions 32-42 in field 90 - Original Data Elements with a default value assigned by Discover.

Discover issuers and acquirers in the US region and in the United Kingdom have the option to participate in the Address Verification Service (AVS).

The Visa Europe System supports the processing of Discover's Cardholder Identification Data (CID) values, which is Discover's version of CVV2. The Visa Europe System accepts the Discover CID from Acquirers and forwards them to the appropriate network and issuers. Acquirers sending in those transactions include field 126.10 - CVV2 Authorization Request Data and American Express CID Data in the requests. Refer to the description of Card Verification Value 2 (CVV2) in the *Visa Europe Technical Service Descriptions*.

If Issuers populate field 62.17 - Gateway Transaction Identifier (bitmap format), and if the Discover acquirer can receive bitmap 62 and chooses to receive field 62.17, the Visa Europe System forwards the field and its contents to the acquirer in the response message.

The Visa Europe System provides reversal processing for Discover transactions. VEAS does not add field 116 to reversals.

### 4.2.8 Plus transactions

The Plus Program is an ATM Card program available to Members worldwide. Plus System, Inc. provides Interchange for Cards bearing the PLUS logo used at ATMs.

Plus transaction flows are the same as those for Visa transactions. Issuers can choose DMSA and DMSC to process their Plus transactions or they can choose SMS.

The Card types in the Plus Program include:

- Visa Cards
- Plus Cards
- Proprietary ATM Cards
- MasterCard cards
- Other credit and debit cards

Plus System, Inc. processes the following ATM Transactions, including their associated reversals and confirmations:

- Withdrawals from checking or savings accounts
- Credit Card cash advances
- Alternative media
- Chip-based transactions

For further information about Plus transactions, refer to the *DMSA Technical Specifications*, and the *SMS ATM Technical Specifications*.

### 4.2.9 Japan Card Network (JCN) transactions

VEAS supports an Authorization Gateway that enables the Japan Card Network (JCN) to pass transactions acquired in Japan to the Visa Europe System for processing. This gateway enables transaction mapping from JCN's format to the V.I.P. format, encryption management, and cryptographic key exchange.

JCN has its own message naming scheme, which differs from Visa's ISO nomenclature. The Visa Europe System reformats incoming transactions from JCN to adhere to Visa's format.

The Visa Europe System supports authorizations, authorization advices, reversals and network management transactions from JCN.

VEAS approves all reversals from JCN in STIP, and sends reversal advices to JCN. This ensures that JCN reversals are processed, and Issuers don't decline them.

### 4.2.10 Reversal request (0400) and response (0410) message flows

Acquirers and Merchants submit a reversal request to cancel part or all of a previously approved transaction or a timed-out authorization.

- Merchants can originate reversals at the POS whenever the Cardholder or the Merchant voids a transaction
- Acquirers can originate reversals when the Acquirer corrects an authorization it processed in error

Only approved Card-based transactions or Authorization Requests that have timed out can be reversed. A reversal should never be used to cancel a decline, a referral, or an Account Verification request.

See Section 4.4.3, *How VEAS processes repeat (duplicate) Authorization Requests*, for further information about timed-out messages.

Figure 10 shows the typical message flow for an Authorization Reversal request.

**Figure 10: Authorization Reversal request message flow - DMSA**

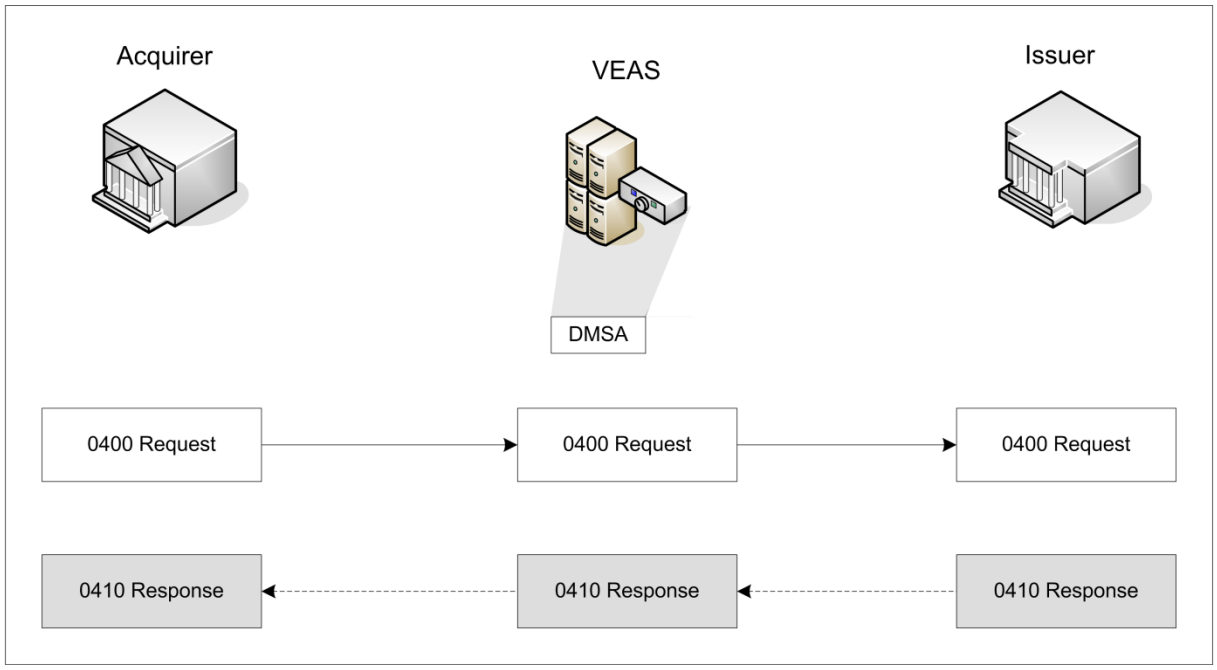
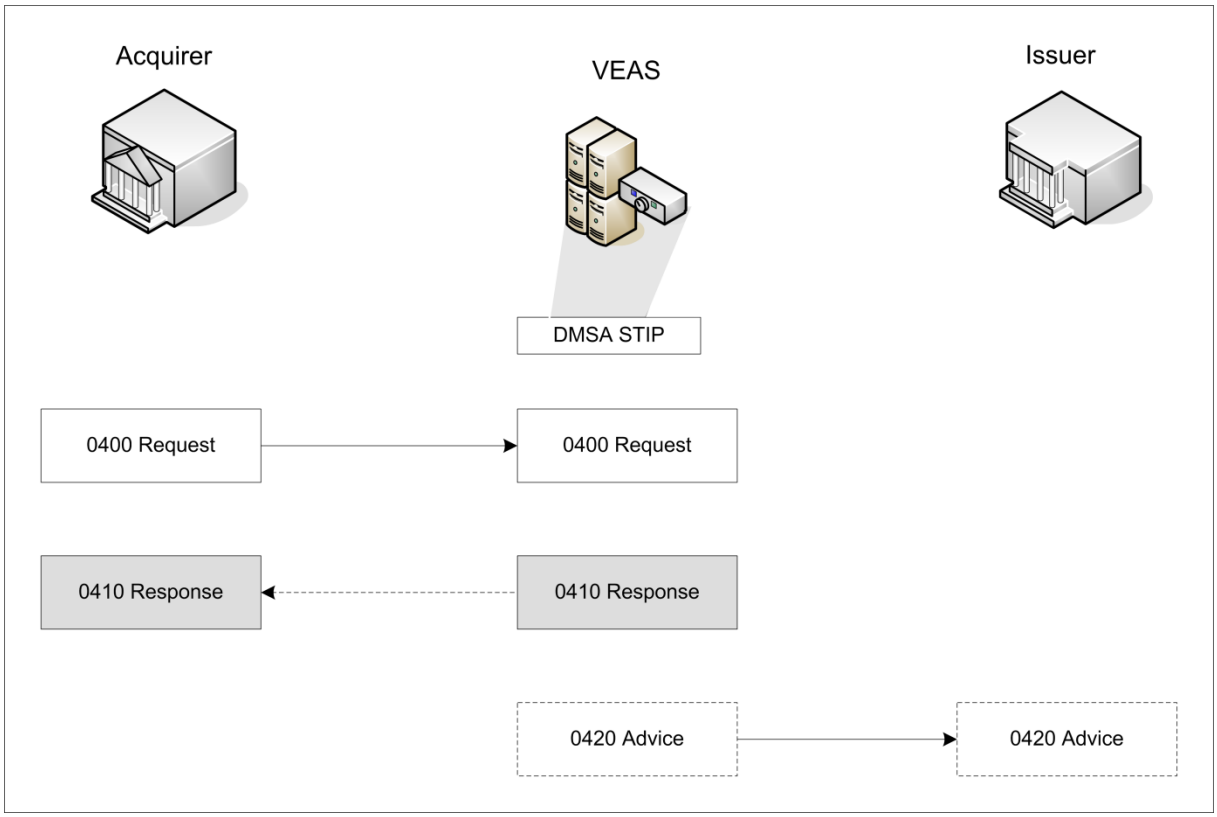



Figure 11 shows the message flow for an authorization reversal request processed by DMSA STIP.

**Figure 11: Authorization Reversal request message flow - DMSA STIP**



Acquirers can use reversals for MasterCard, American Express, Discover, Diners Club, JCB, and private-label Card transactions but cannot use them for:

- Balance inquiries
- 0100 Authorization Requests that were not approved

Depending on the activity present on the Cardholder database (CDB), if STIP declines a reversal, it responds with response code 21 (no action taken) and creates an advice for the Issuer. STIP does not update the Activity File when processing reversals, even if it responds with an approval. See Chapter 8, *Stand-in processing (STIP)*, for more information about reversal processing and about activity checking.

When Issuers process reversals, they should adjust available Cardholder balances.

Reversals can apply to the full original Transaction Amount (full reversal) or to a lesser original Transaction Amount (partial reversal).

### Full reversals

A full reversal completely voids a prior authorization.

Full reversals of POS transactions always contain the original Transaction Amount in field 4 - Amount, Transaction. For multicurrency transactions, the value in field 6 - Amount, Cardholder Billing relates to the reversal's field 4 amount.

Acquirers and Merchants do not include field 95 - Replacement Amounts. If the transaction requires currency conversion, DMSA inserts the converted Transaction Amount in field 6 of the reversal. If the rates change, DMSA inserts the corrected, actual amount in Billing Currency into field 61.2 - Other Amount, Cardholder Billing of the reversal request.

**Note** VEAS converts 0420 SMS full financial reversal messages to 0400 reversal requests for DMSA Issuers.

### Partial reversals

A partial reversal reverses a portion of the original Transaction Amount. Acquirers and Merchants submit a partial reversal when an estimated amount exceeds the final value of the completed transaction. For instance, if the estimated amount is USD 200 but the final amount is USD 100, then a partial reversal can be submitted for the USD 100 difference between the estimated and final amounts.

To process partial reversals of POS transactions, Acquirers and Merchants insert the original Transaction Amount, from field 4 of the original request, into field 4 of the partial reversal. Acquirers and Merchants insert the transaction's corrected, actual amount in field 95. For multicurrency transactions, DMSA ensures that the value in field 6 of the reversal matches the value in field 6 of the original request, unless the conversion rates have changed. If the rates change, DMSA inserts the corrected, actual amount in Billing Currency into field 61.2 - Other Amount, Cardholder Billing of the reversal request.

**Example:**

To reverse USD 20 of a USD 100 transaction, the reversal contains the original amount of USD 100 in field 4 and the corrected amount of USD 80 in field 95. If the transaction requires currency conversion, DMSA inserts the converted original amount in field 6 and inserts the corrected replacement amount, if the currency rates have changed, in field 61.2.

### 4.2.11 ATM Adjustment Messages

ATM Acquirers use 0400 reversals (or 0420 reversal advices) to notify Issuers of ATM malfunctions. If no cash is dispensed, then a full reversal is sent. If the cash dispensed is different from the amount originally authorized, then a 0400 adjustment is sent, which can be for less or more than the amount originally authorized.

The format of the 0400 adjustment is the same as that for a regular partial reversal. Field 4 contains the original authorized amount; field 6 contains the equivalent amount in the Billing Currency of the Cardholder.

The adjusted amount is populated by the Acquirer in field 95 - Replacement Amount; the equivalent replacement amount in the Billing Currency is found in field 61.2 - Other Amount. Cardholder Billing. The replacement amount can only be a greater value than the original amount in ATM adjustments. Non-ATM Transactions that attempt this will be rejected.

DMSA Issuers will always receive ATM adjustments as 0400 reversal requests, even if the Acquirer submitted a 0420 reversal advice. DMSA Issuers will only receive 0420 advices as part of their regular advice processing (that is, if the transaction went to stand-in processing).

SMS Issuers will always receive ATM adjustments as 0220 financial advices, even if the Acquirer submitted a 0400 reversal or 0420 reversal advice. SMS Issuers will only receive 0420 advices if the ATM Transaction was fully reversed.

**Note** Acquirers must not send ATM confirmation (0102) messages to fully or partially reverse ATM Transactions. If attempted, VEAS will reject them with Reject Code 0559 (invalid message type). Acquirers must use 0400 reversal messages to fully or partially reverse ATM Transactions.

### 4.2.12 Automated Fuel Dispenser (AFD) transactions

Acquirers that process AFD transactions must support Partial Authorizations, generate Acquirer confirmation advices, and provide valid transaction amounts to Issuers. This capability ensures the Issuer manages the Cardholder's open-to-buy balance by linking to the Acquirer's confirmation advice.

The AFD transaction flow includes the following:

1. The Acquirer sends an Authorization Request message to the Issuer through VEAS. The message contains:
   - A valid transaction amount up to the maximum Visa Europe amount of EUR 150.00 or local currency equivalent, unless a higher amount is pre-selected by the Cardholder at the pump.
   - The Partial Authorization Indicator.
2. The Issuer approves or declines the Authorization Request and sends a response message to the Acquirer through VEAS. An approval will either be for the requested amount, or if the Issuer supports Partial Authorization, an amount based on the Cardholder's available funds, if less than the amount of the Authorization Request.
3. After the approval message is received by the Acquirer, the fuel is dispensed up to the authorized amount.
4. The AFD then sends the final transaction amount message to the Acquirer.

5. The Acquirer sends a confirmation advice to the Issuer, including the final transaction amount, via VEAS.
6. VEAS acknowledges the message, and the Issuer adjusts the open-to-buy balance.

**Note** If the Issuer is unavailable or has responded with a Partial Authorization when the Partial Authorization Indicator was not set, VEAS will process the Authorization Request in STIP as a full Authorization Request. If the Issuer is set up to receive STIP advices, an advice will be sent regarding the stand-in.

**Important** An Issuer must be prepared for the potential to receive two 0120 advices for the same AFD transaction. This would occur when an Issuer has been certified to receive the 0120 Acquirer confirmation advices in real-time and is also set up to receive STIP advices. In this case the Issuer should use the 0120 Acquirer confirmation advice (identified by a value of **A** in field 44.1) as the final position on the transaction.

### 4.2.13 Transaction Amount (field 4) processing rules

DMSA checks the amount returned by the Issuer in the 0110 response. The value in field 4 must be the same in the request and response unless the Issuer is sending a partial approval. Table 6 shows the new processing rules.

**Table 6: Processing rules for Transaction Amount (field 4)**

| Processing rules for matching preauthorization request with completion message | |
|---|---|
| **Condition** | **Processing rule** |
| An Issuer returns the same amount value that was in the Authorization Request. | Visa Europe accepts the amount in the response and process the transaction. |
| A non-Visa-Europe issuer that does not participate in the Multicurrency Service sends a different amount value in the response with a value of 10 (Partial approval) in field 39 - Response Code. | Visa Europe checks the amount in the response and:<br>■ If the amount is less than the original request, Visa Europe processes the transaction<br>■ If the amount is greater than the amount in the original request, Visa Europe rejects the transaction with reject code 0735 (Partial Authorization field 4 value is greater than the original field 4 transaction amount) |
| An Issuer sends a different amount value in the response and the value in field 39 is not 10. | Visa Europe:<br>■ Rejects the transaction to the Issuer with reject code 0009 (invalid value)<br>■ Processes the transaction in STIP and respond to the Acquirer |

## 4.3 Message flows - Non-authorization

DMSA, Issuers, and Acquirers use non-authorization messages for file maintenance, for administrative requests, and for network management. See Chapter 9, *Non-authorization messages*, for more information.

## 4.4 Message tracking

Both Visa Europe's Authorization Service and Visa Inc.'s V.I.P. System need to be able to track messages inbound and outbound. One or more messages make up a transaction set, for example:

- Authorization Request from Acquirer (Leg 1)
- Authorization Request forwarded to Issuer (Leg 2)
- Authorization Response from Issuer (Leg 3)
- Authorization Response forwarded to Acquirer (Leg 4)

Message tracking is used to ensure that each message is processed in the correct order. In addition, message tracking ensures that responses match requests, that reversals and repeats are processed in the correct sequence, and that transaction messages are not duplicated.

Both VEAS and V.I.P. use a similar technique: an area of memory is set aside for each unique transaction, which is referenced with every message incoming to the system. In VEAS this is known as Context, or the Message Tracking Table (MTT), in V.I.P. it is referred to as the Inter-Task Table (ITT).

If the Issuer does not match certain essential fields in a response, that response will be rejected. For example, if field 11 System Trace Audit Number is different in the response to the original message, the response will be rejected with reject code 0603 (consistency error). As well as checking for consistency, the MTT also monitors response times of each message back from the Issuer.

Although both versions of message tracking have much in common, architectural differences between the VEAS and V.I.P. platforms mean that the behaviour of MTT and ITT varies in a few key respects. These are described in Section 4.4.1, *Key fields used for message tracking*.

### 4.4.1 Key fields used for message tracking

The MTT for both DMSA and SMS messages uses key data elements as an index with every message.

**Table 7: Key data elements for message tracking**

| Key data elements for message tracking | | |
|---|---|---|
| **Key field** | **DMSA** | **SMS** |
| Field 32 - Acquirer Institution ID | M | M |
| Field 37 - Retrieval Reference Number | M | M |
| Field 42 - Card Acceptor ID | C | C |
| Field 41 - Card Acceptor Terminal ID | C | C |
| Field 11 - System Trace Audit Number | - | M |

**Key:**

M = Mandatory index

C = Conditional index (required in subsequent messages if present in the original)

### 4.4.2 System behaviour during message tracking

The system behaviour during message tracking for both DMSA and SMS is summarised in Table 8 and Table 9 respectively.

For SMS processing, transactions are also subject to matching on the Financial Integrity table, to ensure that even if a message itself is correct, that it relates correctly to others in a set of transactions.

**Table 8: System behaviour during DMSA message tracking**

| System behaviour during DMSA message tracking | | | |
|---|---|---|---|
| **Message being processed** | **Last transaction in message tracking** | | |
| | **None** | **Authorization Request** | **Reversal** |
| Authorization Request | F | Discard | Discard |
| Authorization Repeat (0101 only) | F | Discard | Discard |
| Reversal | F | Discard | Discard |
| Reversal Repeat (0401 only) | F | - | - |
| Response | Rej. | F | F |

**Key:**

F = Forward

Rej. = Reject

**Table 9: System behaviour during SMS message tracking**

| System behaviour during SMS message tracking | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Message being processed** | **Last transaction in message tracking** | | | | | | |
| | **None** | **Original** | **Reversal** | **Adjustment** | **Charge-back** | **Charge-back Reversal** | **Representment** |
| Original Request | F | Discard | Rej. | Rej. | - | - | - |
| Reversal Advice | F | Pend | Discard | - | - | - | - |
| Adjustment Advice | F | F | F | Discard | - | - | - |
| Chargeback Advice | F | - | - | - | Discard | - | - |
| Chargeback Reversal Advice | F | - | - | - | - | Discard | - |
| Representment Advice | F | - | - | - | - | - | Discard |
| Response | Rej. | F | F | F | F | F | F |

**Key:**

F = Forward

Rej. = Reject

Pend = Keep until original has completed, then continue

### 4.4.3 How VEAS processes repeat (duplicate) Authorization Requests

DMSA discards a duplicate message if the original is still being processed (that is, DMSA finds an entry in the MTT), logging the discarded duplicate with reason code 006 (Authorization Request in progress). In this context, a discarded message is one that the system does not pass to the output message editor for routing.

**Note** If the Issuer returns a response that does not contain matched MTT key fields from the original request, DMSA rejects the Issuer's response. STIP then processes the transaction according to ATR rules if they apply.

See Section 6.14, *Repeat or duplicate Authorization Requests*, for more information on how Members process duplicate Authorization Requests.

If the request times out, and an Acquirer chooses to retry the Authorization Request, the following messages are required:

- For POS transactions, a repeat or a reversal

  For POS transactions destined for SMS Issuers, SMS Issuers receive 0101 repeat messages as message type 0101. However, VEAS converts 0401 messages from DMSA Acquirers to 0420 messages before forwarding them to SMS Issuers.
- For ATM Transactions, a reversal followed by a new request

  The Visa Europe System does not allow repeats for ATM Transactions. It also does not allow them for any SMS POS or ATM Transaction.

  For ATM Transactions destined for SMS Issuers that do not participate in the ATM Format Conversion Service, VEAS converts 0101 repeat messages from DMSA Acquirers to 0100 messages and converts 0401 messages to 0420 messages before forwarding them to SMS Issuers.

**Note** For ATM Transactions destined for SMS Issuers that participate in the ATM Format Conversion Service, VEAS converts 0101 repeat messages from DMSA Acquirers to 0200 messages and converts 0401 messages to 0420 messages.

**Important** SMS Issuers can potentially receive repeat messages depending on Issuer-selected parameters. If DMSA Acquirers send an 0101 POS request message 10 seconds after the original message has been processed, SMS Issuers receive an 0101 request message.

Visa Europe recommends limiting repeat message submissions to three per request. See Section 4.5, *Undeliverable messages*, for information about how VEAS processes undeliverable requests.

#### 4.4.3.1 Assigning retrieval reference numbers (field 37)

Acquirers must assign a new retrieval reference number for each new 0100 Authorization Request. This number must appear in all subsequent messages related to that transaction. Although Visa Europe recommends against it, Acquirers can use the retrieval reference

number from one transaction in another transaction as long as the first transaction's key information - which includes the field 37 retrieval reference number - is no longer in the MTT. The MTT empties key field information for a transaction when the response to that transaction has been sent by the Issuer or by STIP.

Acquirers must ensure that, for field 37:

- Positions 1-4 contain the same date as in field 7 - Transmission Date and Time in YDDD format where position 1 (Y) = 0-9, and positions 2-4 (DDD) = 001-366
- Positions 5-6 contain the hours from field 7 in hh format
- Positions 7-12 contain the value from field 11 - System Trace Audit Number in nnnnnn format

**Important** Acquirers must not reuse the same value in the last six positions of field 37 in another transaction within the same calendar day. Otherwise, DMSA may reject the message with reject code 0094 (invalid value in first four digits).

## 4.5 Undeliverable messages

DMSA performs specific procedures for requests that are not eligible for STIP and for responses when they cannot be delivered to their destinations.

### 4.5.1 Undeliverable requests ineligible for STIP

When DMSA is unable to deliver an Authorization Request and cannot invoke STIP, it initiates a response containing response code 91 (Issuer Processor or switch inoperative). DMSA uses response code 91 for requests destined for other networks or systems, or, at the Issuer's option, for undeliverable Card-not-present authorizations, for instance, mail order/telephone order (MOTO) transactions, or Electronic Commerce Transactions. When Acquirers receive a response message containing response code 91, they may retry the request or may use a downtime procedure (if the centre has developed one). Centres should submit retries every 30 minutes.

For time-outs, if Acquirers choose not to retry the request, they must use a reversal to close out the transaction set.

**Note** When an Acquirer reverses an Authorization Request, Issuers should ensure that they have identified the original request before reinstating the Cardholder's credit limit.

If a request times out and the Acquirer chooses to retry the Authorization Request, Visa Europe requires the following messages:

- For POS transactions, either a repeat or a reversal followed by a new request.

  For POS transactions destined for SMS Issuers, SMS Issuers receive 0101 repeat messages as message type 0101. However, VEAS converts 0401 messages from DMSA Acquirers to 0420 messages before forwarding them to SMS Issuers.
- For ATM Transactions, a reversal followed by a new request. VEAS does not allow repeats for ATM Transactions, or for SMS POS transactions or ATM Transactions.

  For ATM Transactions destined for SMS Issuers that do not participate in the ATM Format Conversion Service, VEAS converts 0101 repeat messages from DMSA Acquirers

to 0100 messages and converts 0401 messages to 0420 messages before forwarding them to SMS Issuers.

For ATM Transactions destined for SMS Issuers that participate in the ATM Format Conversion Service, VEAS converts 0101 repeat messages from DMSA Acquirers to 0200 messages and converts 0401 messages to 0420 messages before forwarding them to SMS Issuers.

**Important** SMS Issuers can, potentially, receive repeat messages depending on Issuer-selected parameters.

**Note** Acquirers should ensure that their Merchants know to re-read the Card when resubmitting an Authorization Request after the previous request has been reversed.

Except for their message designator (for instance, 0101 or 0401), repeat messages are copies of the originals and therefore are the same as the original messages, containing the same values.

### 4.5.2 Undeliverable responses from Issuers

If DMSA cannot deliver an authorization or reversal response to an Acquirer, it returns the response to the Issuer. When DMSA returns a response, it reverses the source and destination identifiers in the message header and changes the value in the returned message flag in the header to 1, indicating that this is a returned message.

Figure 12 illustrates an example of a returned message.

**Figure 12: Returned message example**


1. DMSA sets the value to 1 in header field 9, byte 3, bit 1. The rest of the message is unchanged.

An Issuer can discard a returned response. Special action is not needed because the Acquirer sends a repeat request if it does not receive a response from the Issuer.

If the Issuer participates in ATR), STIP then processes the transaction according to ATR rules and settings.

If the Issuer returns a response that does not contain matched MTT key fields from the original request, DMSA discards the Issuer's response. For instance, if the value in field 11 in the response message does not match the one in field 11 stored in the MTT, VEAS rejects the response with Reject Code 0603 (consistency error response and request). STIP then processes the transaction according to ATR settings.

**Note** The Message Tracking Table (MTT) is an internal table within VEAS that VEAS uses to temporarily store messages so it can match requests to responses and monitor response times.

For further key field information, see Section 5.8, *Addition to the Message Tracking Table*, and the *DMSA Technical Specifications*. See also Section 4.4.3, *How VEAS processes repeat (duplicate) Authorization Requests*, for repeat or duplicate message processing information. Further ATR information is in Chapter 5, *Initial message parsing and editing*.

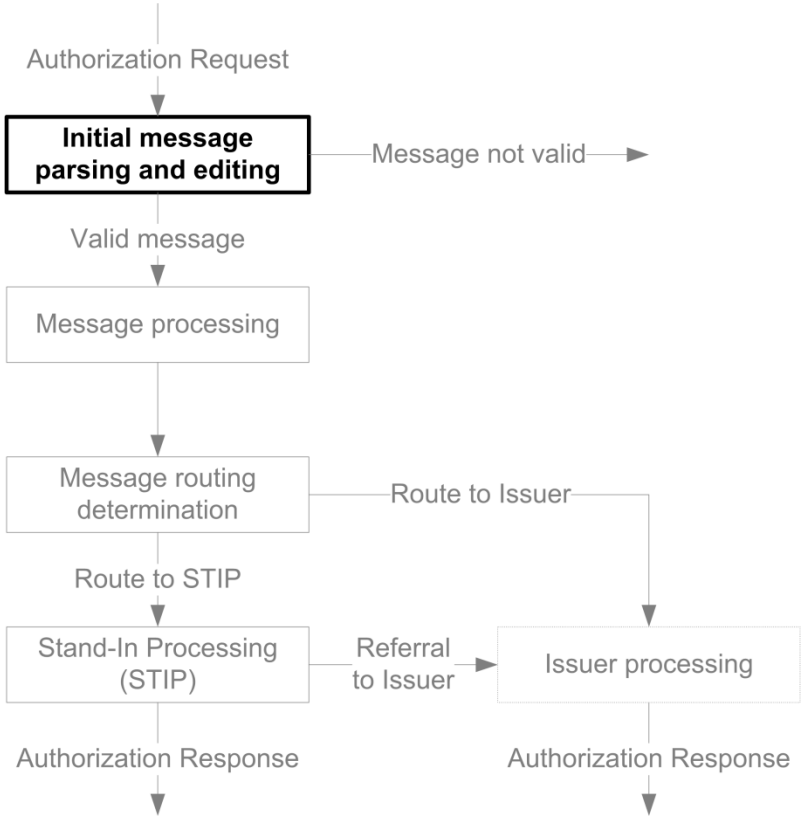
# 5 Initial message parsing and editing

DMSA validates an Authorization Request message from the Acquirer and prepares it for processing. These validation and preparation functions include identifying the message, determining the Issuer Processor's instructions for the message type, validating the message format, and editing field content. Every message must comply with the message requirements specified in the *DMSA Technical Specifications*. DMSA also performs any Issuer-specified services such as adding the Optional Issuer Fee for multicurrency transactions or validating PINs.

## 5.1 Where initial message parsing and editing fits into the overall DMSA process

Figure 13 illustrates where initial message parsing and editing fits into the overall DMSA process.

**Figure 13: Initial message parsing and editing**




## 5.2 Overview of message parsing and editing

The tasks involved with this phase of DMSA processing include:

- Converting PIN data from 8 bits to 16 bits, if necessary
- Classifying the transaction message, for instance, as a request or as a response
- Obtaining Acquirer and Issuer profiles from the system tables
- Checking and editing message fields

- Performing the Visa Smart Debit/Credit (VSDC) Service, or CPS functions, or validating a Cardholder Authorization Verification Value (CAVV) in an electronic commerce (e-commerce) request

For information about CPS/ATM, refer to the description of Custom Payment Service/ATM see the *Visa Europe Technical Service Descriptions*.

Currently, there are no CPS/POS programs running within the Visa Europe Territory. These programs may however be utilised by Processors running cross-border activities. For more information, please refer to the V.I.P. system manuals.

### 5.2.1 Summary of functions performed by DMSA on requests from Acquirers

The first functions that DMSA performs on requests from Acquirers are described in subsequent sections. They apply to all authorization-related Cardholder transactions processed by DMSA, including electronic commerce (e-commerce) transactions:

- Message source validation and message logging:
  - Verifying message source
  - Validating the Acquirer BIN
  - Logging message and performing administrative tasks
- Message parsing and pre-routing message editing:
  - Converting PIN data if required
  - Classifying the transaction message
  - Obtaining Acquirer and Issuer profiles from system tables
  - Editing message fields
  - Performing any service processing, such as that for Real-Time Scoring (RTS) or for the Custom Payment Service (CPS)
- Currency conversion
- Adding messages to the Message Tracking Table (MTT) for tracking and response time purposes
- Starting Positive Cardholder Authorization Service (PCAS) processing
- Determining message destination
- Determining message routing
- Performing any magnetic stripe-based Card Verification Value (CVV), Integrated Card Verification Value (iCVV), Card Verification Value 2 (CVV2), Cardholder Authentication Verification Value (CAVV), Dynamic Card Verification Value (dCVV), or PIN Verification Value (PVV) security module functions
- Performing any functions for contactless transactions

Under PCAS control, DMSA then routes the message to stand-in processing (STIP) or to the Issuer. If the message is going to the Issuer, DMSA starts the Assured Transaction Response (ATR) timer.

**Note** The ATR Service provides for additional response time for online PIN based transactions.

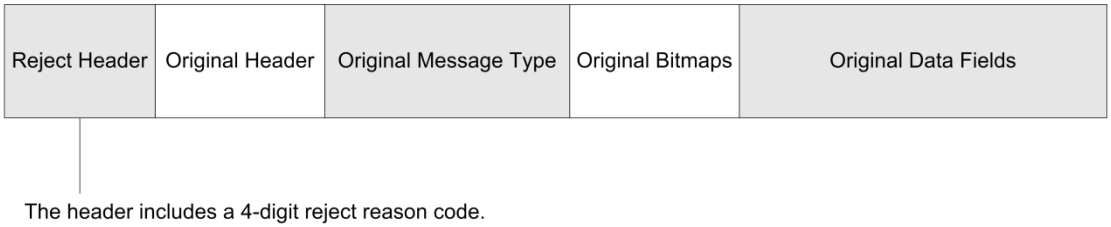
### 5.2.2 Rejected messages

If DMSA encounters a condition at any point in the process that precludes further processing, DMSA rejects or declines the message back to the Acquirer or forward-refers the message to the Issuer for disposition.

DMSA rejects a message if it detects an error that should have been detected by the originator of the message. For instance, the message contains an alphabetic character in a numeric field or does not contain a required field.

When DMSA rejects a message, it returns the message unchanged to the sender, but precedes the message with a reject message header. The reject message header contains a reject code that identifies the error, as shown in Figure 14.

**Figure 14: Rejected message example**



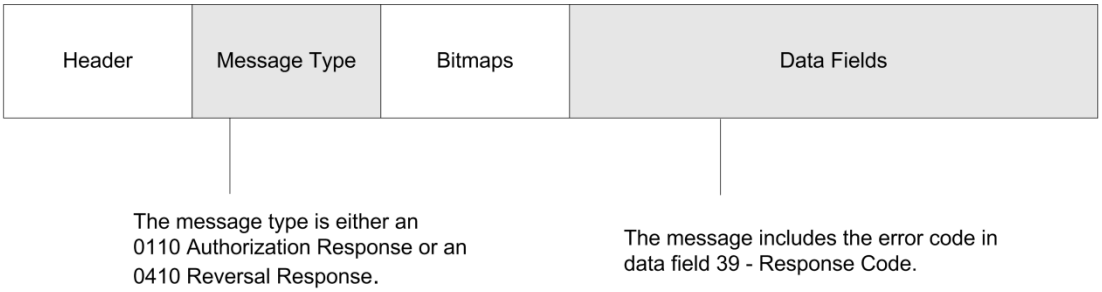

The reject header contains the standard header data plus two extra fields: a bitmap (in header field 13) and a 4-digit code (in header field 14) that identifies the reject reason. For valid reject codes, refer to the *DMSA Technical Specifications*.

DMSA can reject a message from a Processing Centre, but a Processing Centre cannot reject a message originating from DMSA.

DMSA declines a request for authorization or financial service with an error response code if the error condition is one that the message originator is not expected to detect; for instance, the Account Number of the Card does not belong to any known Issuer.

DMSA generates a Decline Response message, as indicated in Figure 15.

**Figure 15: Decline Response example**




The *DMSA Technical Specifications* identify valid error Decline Response codes.

### 5.2.3 Global processing mandate

Processing uniformity is essential to establish a consistent set of processing results. These processing capabilities are designed to improve the identification of transactions.

The global processing mandate is as follows:

- All Acquirers and Issuers must support the Transaction Identifier (TID) field 62.2 in all Exception Transactions

- All Acquirers must support lifecycle processing by including the TID in all original transactions
- All Acquirers must demonstrate the ability to send the Merchant Verification Value (MVV) field in all related Visa Europe System transactions, including authorization messages, clearing and settlement transactions, and Exception Transactions
- All Issuers must demonstrate the ability to retain and return the MVV field in all Exception Transactions

## 5.3 Message source validation and message logging

When DMSA receives an Authorization Request, it uses information in the request along with information in the system tables to determine the originator of the request, including the information in Table 10.

**Table 10 Information used to determine the originator of the request**

| Information used to determine the originator of the request | |
|---|---|
| **Request information** | **System table information** |
| Source Station ID (header field 6) | Acquirer EA Server station address |
| Acquirer's BIN (field 32) | Acquirer BIN Control Record (BCR) and Processing Centre Record (PCR) |
| Acquirer's country code (field 19) | |

For detailed field descriptions, refer to the *DMSA Technical Specifications*.

### 5.3.1 Verifying message source

Verifying the message source involves determining the Acquirer's country code, and the Acquirer's and Merchant's region codes. The fields DMSA uses in this process are:

- Field 19 - Acquiring Institution Country Code
- Field 32 - Acquiring Institution Identification Code
- Field 33 - Forwarding Institution Identification Code
- Field 43 - Card Acceptor Name/Location

To determine the Acquirer's country code, VEAS first looks to field 43. If field 43 is not present in the request, or if the country code in field 43 is incorrect when VEAS compares it to the system's list of valid country codes, VEAS then uses the field 19 country code.

To determine the Acquirer's region code, VEAS uses the field 19 country code. If field 19 is not present in the message, VEAS uses field 32 to locate the Acquirer's BIN Control Record (BCR), and uses the default country value in that BCR. If field 19 is not present, and the Acquirer's BCR is not available, VEAS uses the Acquirer's Processing Centre Record (PCR).

**Note** If the Acquirer region code is already specified in message header field 9, the message was acquired by SMS.

To determine the Merchant's region code, VEAS uses the country code in field 43. If field 43 is missing, the system uses the Acquirer's region code.

**Note** Authorization Requests for ATM Cash Disbursement require fields 41, 42, and 43. For field presence requirements in POS Authorization Requests, refer to the field 41, 42, and 43 descriptions in the *DMSA Technical Specifications*.

**Note** For Authorization Requests that contain PIN data (in field 52 - Personal Identification Number (PIN) Data and in field 53 - Security-Related Control Information), VEAS uses field 32 to identify the source of the Acquirer Working Key (AWK). If field 33 is also present, the system uses that Acquirer identifier as the AWK source rather than using the Acquirer identified in field 32.

VEAS routes transactions to Issuers based on the Account Number range unless field 100 - Receiving Institution Identification Code (for certain non-Visa card transactions), or field 121 - Issuing Institution Identification Code (for non-ISO-standard Account Numbers) is present. If present, VEAS uses the values in those fields for routing. Acquirers must first clear the use of those fields with Visa Europe. See Section 5.9, *Determination of message destination*.

So that billing processing can distinguish cross-border-issued transactions for Visa Commercial Card programs, DMSA always logs the BIN country as a point of comparison. For instance, a UK Issuer that issued a Card in France would have a BIN country code of 826 but an ARDEF country code of 250; a Card issued in the UK by that same UK Issuer would have a BIN country code of 826 and no ARDEF country code.

### 5.3.2 Logging messages and performing administrative tasks

After DMSA validates the message's source, the system logs the request. DMSA logs each request and each response message to compile data for billing, preparing reports, recovering files, and researching problems.

Members and Processors can view completed authorization transactions by accessing the logs made available to the VTRS and VROL systems. Incomplete authorizations, such as those that were returned or rejected, may not appear in these logs. Members and Processors are therefore encouraged to ensure that their systems capture returned/rejected messages for later analysis.

VEAS does capture the full content of entire messages - including all fields to/from both the involved Processors - which is used for Member testing and problem research. However, VEAS does not match entire reversals to entire original authorization messages.

## 5.4 Message parsing

### 5.4.1 PIN translation

For messages containing PINs, the Visa Security Module (VSM) converts the PIN format and the presentation to a format and a presentation that the Issuer can interpret. The presence of field 52 - Personal Identification Number (PIN) Data and field 53 - Security-Related Control Information in a request indicates that the message includes PIN data. This PIN formatting (or translating) task is not the same as the PIN Verification task that the PIN Verification Service (PVS) performs.

VEAS either forwards field 52 and field 53 to the Issuer or drops them from a request message depending on which PIN Verification option the Issuer chooses.

If the Issuer chooses to have both VEAS and its own Processor perform verification, and when the Issuer is available to verify PINs, VEAS performs PIN translation and forwards field 52 and field 53 to the Issuer for PIN Verification. When the Issuer is unavailable, the Visa Europe System forwards the two PIN fields to STIP for translation and verification.

If the Issuer chooses to have VEAS perform PIN Verification and if PIN Verification is successful, VEAS drops field 52 and field 53 from the request message to the Issuer.

### 5.4.2 Message classification

Classifying a transaction message includes determining whether it is a request or a response and whether the transaction code is valid. DMSA also retrieves the appropriate message template, for instance, an 0100 purchase template.

DMSA edits transactions for message validity, that is, a transaction set cannot include invalid messages. For instance, a Cash Disbursement transaction cannot include a balance inquiry message.

DMSA rejects any message that is out of context (or out of sequence) to prevent it from being sent to Issuers.

### 5.4.3 Obtaining Acquirer and Issuer profiles

DMSA checks its system tables for Member-defined processing parameters, such as the BCR, Issuer limits, the Issuer's Risky Countries table, various Card program restrictions, and default response codes used in STIP. The system tables also contain service options, for instance, participation in Real Time Scoring. DMSA uses this information to perform subsequent tasks. Section 6.4, *Risk level and limits determination*, describes the Risky Countries feature. See Section 8.4.1, *Determine default response code*, for a list of allowable default response codes that the Issuer can specify.

## 5.5 Editing message fields

DMSA examines and edits message fields to ensure that they contain valid:

- Formatting, for example, that the Card expiry date is in YYMM format
- Syntax, for example, if a field requires a leading asterisk
- Content, for example, the value in field 4 - Amount, Transaction is zeros when it should contain an amount
- Inter field relationships; DMSA compares different fields within a message to make sure that there is not any conflicting information
- Service-specific field information; for example, if the Acquirer subscribes to CPS, DMSA validates the contents of field 62 - Custom Payment Service Fields

When DMSA finds invalid data in a field (for instance, a zero when the value must be a non-zero numeric), it returns the message to the Acquirer. When DMSA finds data conflicts between related fields, it can return the message to the Acquirer, send the message to STIP, or forward the message to the Issuer to be resolved, based on options that the Issuer selects.

If DMSA finds an error in one of the key CPS fields in a message being submitted for CPS qualification but the message is otherwise valid, DMSA downgrades it to a less advantageous reimbursement level and continues processing.

**Example:**

If the authorization characteristics indicator (ACI) in field 62 is not one of the allowable values, DMSA downgrades the request and processes it as a non-CPS-qualified transaction.

**Note** VEAS will assign a TID in field 62.2 - Transaction Identifier (Bitmap Format) to all POS and ATM dual- and single-message transactions regardless of whether the transactions have been submitted for CPS consideration, including preauthorization messages and V.I.P. message format Plus transactions.

Basic processing rules that govern Authorization Requests dictate DMSA editing criteria. These rules specify the requirements, the restrictions, and the use of the fields containing the following information:

- Account Numbers
- Processing codes
- Magnetic stripe data
- Chip data
- Transaction Amounts
- Free text in authorization messages
- Expiry dates

For every message, DMSA performs edits on these fields as described in the following sections.

### 5.5.1 Editing Account Numbers

All POS and ATM Card authorization messages require an Account Number. DMSA determines if the Account Number is valid and returns the message to the Acquirer if:

- The Account Number is not the same in all messages in a set for a given transaction
- The Account Number is missing
- The Account Number length does not correspond to the allowable Account Number lengths defined in the Issuer's system tables

  Members specify valid Card lengths for specific BINs in an account range definition (ARDEF).
- The field entry is all alphabetic characters
- The Account Number in field 35 - Track 2 Data is missing or does not match the Account Number in field 2 - Primary Account Number

  This requirement applies to Visa Card POS transactions and ATM Transactions (network 0002). It does not apply to Plus ATM transactions (network 0004).

Typically, Account Numbers of Cardholders are unique ISO-standard Account Numbers that include the Issuer ID in the first six positions. DMSA supports the following types of Account Numbers:

- 13- or 16-digit numeric bank Card numbers

  DMSA currently uses only the Luhn modulus-10 check digit algorithm to verify the check digit. Only STIP performs this verification.

- 19-digit numbers for VPAY
- 5-28-digit numeric bank Card numbers and Proprietary Card numbers
- 5-15-character alphanumeric private-label Card numbers

There are four fields that can contain the Account Number of a Cardholder. The field used depends on the Issuer and on the Card program. These fields are:

- Field 2 - Primary Account Number
- Field 102 - Account Identification 1
- Field 103 - Account Identification 2

Standard Account Numbers 7-19 digits in length go in field 2 of the request.

**Note** Members that want to use Account Numbers with fewer than 19 numeric digits or that are non-ISO standard must first consult with Visa Europe to determine the fields to use for Account Number and Issuer identification.

Acquirers use fields 102 and 103 for proprietary or private-label Account Numbers that include alphabetic characters or that are otherwise non-standard. If field 102 or field 103 appears in the message, the message also must include field 121 - Issuing Institution Identification Code. For details about using field 121, refer to the *DMSA Technical Specifications*. Members must prearrange the use of fields 102 and 103 with Visa Europe, which assigns the ID code to be used in field 121.

Acquirers supply field 100 - Receiving Institution Identification Code to identify the Issuer when they cannot specify the message destination in any of the fields (2, 102, 103, and 121).

The content is typically a 6-digit, Visa-assigned BIN.

### 5.5.2 Editing processing codes

All Authorization Requests must contain a processing code in field 3 - Processing Code that identifies the transaction type and the type of customer account that it affects. The processing code indicates which of the following transaction types the Authorization Request is for:

- Purchase of goods or of services
- Cash withdrawal or advance
- Quasi-cash (for instance, a money order or a wire transfer)
- Available funds inquiry for the Cardholder's account or credit balance
- Visa Commercial Card large ticket
- PIN change or PIN unblock

The processing code also identifies the customer account type that is affected by the transaction. Customer account types can include checking, savings, Credit Card, and universal accounts, or spending power. For detailed information about valid processing codes and about coding requirements, refer to the *DMSA Technical Specifications*.

### 5.5.3 Editing condition codes

A value of 71 in field 25 - POS Condition Code indicates a key entered POS transaction at a US Acquirer. The Visa Europe System does not use this value.

If a transaction is received from an Acquirer with field 25 set to the value 71, VEAS converts this value to 00.

### 5.5.4 Editing magnetic stripe and service restriction code data

DMSA checks to make sure that the Card's magnetic stripe data appears in the Track 1 and Track 2 fields of the Authorization Request. For content requirements of the track data in fields 35 and 45 in Authorization Request messages, refer to *the DMSA Technical Specifications* and to the *Payment Technology Standards Manual*.

### 5.5.5 Service restriction code check

DMSA validates any magnetic stripe-based Service Code identifying Card restrictions specified by the Issuer or that apply to the Card type. For instance, Issuers can restrict the geographic locations at which their Cards can be used by specifying parameters for Merchant categories or for country codes. If the validation fails, DMSA responds with response code 57 (transaction not permitted to Cardholder) in field 39 - Response Code.

The Issuer's system tables can include a list of countries in which Cards associated with a given BIN can (or cannot) be used. To avoid the possibility of conflicting Service Code values, Acquirers must not include field 40 - Service Restriction Code in requests because the field is not valid and it may conflict with the service restriction code in the magnetic stripe data.

For Visa Cards, refer to the Service Code definitions in *the Payment Technology Standards Manual*.

### 5.5.6 Editing Transaction Amounts

Amounts in authorization messages are expressed in:

- The currency of the Merchant/Acquirer; and
- The Cardholder billing currency/Issuer currency.

The amount values in this manual are expressed in USD, and used as a default base currency in VEAS. Transactions in currencies other than USD are converted using Visa's most recent exchange rates to determine if the transaction falls within the USD maximum amount.

### 5.5.7 Visa Europe Transactions

For Visa Europe Transactions processed by VEAS and VECCS, the maximum amounts that DMSA allows for POS transactions are:

- For Visa Signature Preferred and Visa Infinite: USD 999,999.99
- For Visa Signature, commercial and small business products: USD 749,999.99
- For all other card products: USD 499,999.99

The amounts include charges and fees, such as optional Issuer fees. Acquirers must contact Issuers to obtain authorizations for larger Transaction Amounts.

### 5.5.8 International Transactions

For International Transactions, where only the Issuer or the Acquirer, but not both, are within Visa Europe, the maximum amounts that DMSA allows for POS transactions range from USD

99,999.99 to USD 999,999.99, depending on Card product and whether the transaction is POS, ATM or a Manual Cash Disbursement.

### 5.5.9 Visa Europe Commercial Large Value Transaction Program

The Visa Europe Commercial Large Value Transaction Program is only available for Cards where the account ranges have been registered with the program. The program supports large value payments for Visa Commercial credit, charge and deferred debit Issuers. It enables Acquirers and Issuers to process large value POS transactions that are greater than USD 749,999.99 and less than USD 9,500,000.00 or a local currency equivalent.

The program is offered either as domestic or within the Territory. It is not offered for International Transactions that involve interactions between Visa Inc. and Visa Europe.

The Visa Europe Commercial Large Volume Program supports:

- Transactions of value greater than USD 749,999.99 and less than USD 9,500,000.00 or local currency equivalent
- Dual message transactions
- Card-not-present transactions only
- Transactions processed by Visa Europe Systems
- Visa Commercial credit transactions
- Transactions that are domestic or within the Territory

Table 11 lists the types of Cards and transaction limits supported by the program.

**Table 11 Card products and transaction limits supported by the program**

| Product ID | Description | Funding source | Transaction limits (equivalent to USD) | |
|---|---|---|---|---|
| | | | Existing | Commercial Large Value Transaction Program |
| G | Visa Business | C (Credit)<br>H (Charge)<br>R (Deferred debit) | Less than 750,000.00 | Greater than 749,999.99 and less than 9,500,000.00 (or local currency equivalent) |
| K | Visa Corporate T&E | | | |
| S | Visa Purchasing | | | |

### 5.5.10 Travel & Entertainment (T&E) Transactions, large ticket

T&E Transactions can be submitted as commercial large ticket transactions if the issuing BIN is participating in the program.

The maximum amount for T&E Transactions is USD 9,999,999.99, including any charges and fees, when the ARDEF participation flag (large ticket) is ON for the Card number.

This applies for the following Card products: Visa Business, Visa Corporate, Visa Business Check Card, Prepaid Commercial, Visa Purchasing, Visa Purchasing with Fleet, Visa Purchasing GSA, and Visa Purchasing GSA with Fleet.

### 5.5.11 Global Visa Purchasing Large Ticket Program

Visa supports certain transactions up to a maximum USD 9,999,999.99.

The Global Visa Purchasing Large Ticket Program is available to Issuers outside the Territory that meet certain credit settlement risk and anti-money laundering criteria. Acquirers can submit Authorization Requests with higher transaction limits. These limits apply to Visa credit and debit Cards, and exclude Visa prepaid products. Card-not-present, as well as Card-present purchase transactions qualify, including their reversals, credit vouchers, and exception items.

The following MCCs are excluded:

4829 (wire transfer money orders)

6010 (manual cash disbursements)

6011 (ATM cash disbursements)

6012 (account funding – financial institution)

6051 (account funding – non-financial institution)

6211 (security brokers/dealers)

7800 (government owned lotteries)

7801 (government licensed casinos (online gambling))

7802 (government licensed horse/dog racing)

7995 (betting, including lottery tickets, casino gaming chips, off-track betting, and wagers at race tracks)

### 5.5.12 Additional information

STIP does not process commercial large ticket POS transactions between USD 99,999.99 and USD 10,000,000.00. The Visa Europe System sends transactions with amounts in that range to available Issuers; STIP responds with response code 91 (Issuer unavailable) for Issuer-unavailable transactions or when transactions are timed out according to Assured Transaction Response (ATR) settings. STIP processes commercial large ticket POS transactions under USD 100,000.00 using regular Issuer-specified processing rules.

The amount in field 4 - Amount, Transaction must be identical in all request and response pairs that require the field. Amount consistency requires that approvals must be for the amounts requested.

**Note** The rule that the value in the response or advice must match the amount in the request does not apply to partial approval transactions.

### 5.5.13 Editing free-text data

Visa Europe does not recommend that Acquirers insert free text in field 48 - Additional Data - Private of an authorization message because the text may delay processing or may be ignored by the Issuer. DMSA STIP ignores free text when it processes Authorization Requests. If Acquirers must include text in an Authorization Request, they should make the first character an asterisk to distinguish it as user text.

### 5.5.14 Editing expiry dates

All Card-present Authorization Requests must contain a month and year Card expiry date. For Card-not-present transactions such as mail order/telephone order (MOTO) transactions, or Electronic Commerce Transactions, Acquirers must enter the date in field 14 - Date, Expiration of the request message if:

- The expiry date is known
- The Issuer has set its BIN-level option to prevent requests from being processed without expiry dates

VEAS considers a field 14 expiry date to be expired if it is 50 years greater than the current date.

Issuers of Visa Cards must use valid expiry dates. DMSA does not allow special substitute dates such as 1111 or 2222. DMSA interprets the value 1111 as November 2011.

DMSA checks to make sure the date format is YYMM where YY = 00-99 for the year, and MM = 01-12 for the month. Members should not alter the expiry date in magnetic-stripe-read transactions.

Plus Issuers may use the value 4912 to designate a non-expiring Card.

**Note** For transactions from SMS Acquirers to DMSA Issuers that lack an expiry date in field 14 but contain a magnetic stripe in field 35 - Track 2 Data, VEAS inserts the date from the magnetic stripe in field 14 in the message. Conversely, VEAS does not remove field 14 from requests from DMSA Acquirers to SMS Issuers that include track data.

See Chapter 8, *Stand-in processing (STIP)*, for the procedures that STIP uses to determine the expiry date.

### 5.5.15 Performing service or technology-specific processing

Depending on the Member profile, DMSA executes chip processing for the VSDC Service, the CPS, or the Visa Secure Electronic Commerce (VSEC) Service.

## 5.6 Determination of Merchant Category Group

Merchant Category Groups (MCGs) are collections of similar Merchant types that Issuers use to specify processing parameters.

DMSA has defined 11 MCGs to enable Issuers to specify processing parameters according to the varying risk and customer service implications of different Merchant or transaction environments. Each MCG has its own set of related Merchant Category Codes (MCCs) that designate a given business or service. The MCC appears in the Authorization Request message in field 18 - Merchant Type to classify the message in one of the MCGs.

For a complete list of Visa-supported MCCs, refer to the *Merchant Data Standards*.

MCGs are grouped into two major categories: Purchases and Cash. The Purchases category, also known as Non-Cash, consists of two subgroups: T&E and Purchases. Table 12 shows the transaction categories, transaction types, and their indicators and names.

**Table 12: Merchant Category Groups**

| Merchant Category Groups | | | |
|---|---|---|---|
| **Transaction category** | **Transaction type** | **MCG indicator** | **Merchant Category Group (MCG) name** |
| Purchase | Travel & Entertainment (T&E) | 1<br>2<br>3<br>4 | Commercial Travel (Airline)<br>Lodging<br>Auto Rental<br>Restaurant |
| | Purchases (Non-T&E) | 5<br>6<br>7<br>11 | MOTO/e-commerce<br>Risky Purchase<br>Other Purchase<br>Medical |
| Cash | Cash | 8<br>9<br>10 | Other Cash<br>ATM<br>Quasi-Cash |

DMSA manages MCGs and stores them in the DMSA system tables. Once it identifies the MCG, DMSA can determine how to handle the request with respect to the Issuer-specified limits, Issuer-available and Issuer-unavailable conditions, and other risk control factors that the Issuer may have specified.

The MCG index is internal to VEAS. Table 13 lists the internal MCG indicators.

**Table 13: Merchant Category Group index**

| Merchant Category Group index | |
|---|---|
| **Name** | **Index** |
| Commercial Travel (Airline) | 1 |
| Lodging | 2 |
| Auto Rental | 3 |
| Restaurant | 4 |
| MOTO/e-commerce | 5 |
| Risky Purchase | 6 |
| Other Purchase | 7 |
| Other (Manual) Cash | 8 |
| ATM | 9 |
| Quasi-Cash | 10 |
| Medical | 11 |

### 5.6.1 Key message fields for determining MCGs

DMSA determines the applicable Purchase or Cash MCG based on the values in the following message fields:

- Field 3 - Processing Code

  This indicates the transaction type, for instance, a POS purchase transaction or a cash withdrawal.

- Field 18 - Merchant Type

  This is a required field in all authorization and reversal requests that contains the MCC describing the Merchant's type of business product or service.

  - If a transaction does not include field 18, DMSA sets the MCG to Other Purchase
  - If the field 3 processing code indicates Account Funding (10), DMSA sets the MCG to Quasi-Cash. DMSA also uses the Quasi-Cash MCG for existing debt transactions and for online (Internet) gambling
  - For secure e-commerce transactions (field 25 contains 59), DMSA sets the MCG to MOTO
  - If the Issuer is non-US and field 18 contains 4411 (Cruise Line) or 4112 (Passenger Railway), DMSA sets the MCG to Other Purchase (07)

- Field 25 - Point-of-Service Condition Code

  This is a required field in all authorization and reversal requests that identifies the conditions at the point-of-service. For instance, 00 indicates a normal transaction and 08 indicates a Card-not-present MOTO/e-commerce Authorization Request. In some cases, DMSA converts the Point-of-Service Condition Code supplied by the Acquirer. For instance, for e-commerce transactions, DMSA converts Point-of-Service Condition Code 59, which signifies e-commerce, to 08 for Issuers that are not certified for Visa Secure Electronic Commerce (VSEC) programs.

- Field 52 - Personal Identification Number (PIN) Data

  If present in a request, this contains an encrypted Cardholder PIN or password. ATM Cash Disbursements, ATM balance inquiry requests, and UK – domestic PIN change or unblock requests always require field 52.

Table 14 lists the exceptions to determining MCGs.

**Table 14: Exceptions to determining MCGs**

| Exceptions to determining MCGs | |
|---|---|
| **If…** | **Then MCG is set to** |
| Field 18 is not present | Other Purchase |
| Field 3.1 contains 10 (Account Funding), or if the transaction is for an existing debt | Quasi-Cash |
| Field 3.1 contains 01 (Cash Disbursement) and the Merchant Type is not ATM | Other Cash |
| Field 25 contains 08 (mail order) or 59 (e-Commerce) and the MCG determined from field 18 is not Travel/Airlines | MOTO |

| Exceptions to determining MCGs | |
|---|---|
| **If…** | **Then MCG is set to** |
| Field 18 contains 4411 (Cruise Line) or 4112 (Passenger Railway) and the Issuer is non-US | Other Purchase |

### 5.6.2 Determination of default response for MCGs

Issuers can specify two sets of default response codes for a BIN for STIP to use during stand-in processing: one set for when the Issuer is available, and another set for when the Issuer is unavailable. Issuers can specify separate response codes for each MCG. During stand-in processing, DMSA evaluates the Issuer-specified default response code and the STIP-generated response code, and chooses the more severe of the two.

Valid default response codes are:

- 00 - Successful approval or completion
- 01 – Refer to Issuer
- 04 - Pick up Card
- 05 - Do not honour
- 57 - Transaction not permitted to Cardholder
- 86 - Unable to verify PIN
- 91 - Issuer unavailable or switch inoperative (STIP is not applicable or available)

If the response code is 57, DMSA blocks the transaction and does not create an advice.

## 5.7 Currency conversion

DMSA performs currency conversion when the Transaction Currency is different from the Billing Currency of the Cardholder.

DMSA uses the Multicurrency Service to convert currency when it receives messages containing two or more currencies in either of the following fields:

- Field 4 - Amount, Transaction
- Field 6 - Amount, Cardholder Billing

DMSA adds the conversion rate it uses to the request. VEAS then performs a conversion of the amount and source currency to the destination Billing Currency using the conversion rates associated with the transaction type as specified by the processing code.

Participation in the Multicurrency Service is mandatory for Visa Europe members.

**Note** Some registered Merchants can perform currency conversion locally, and they submit transactions in the Billing Currency of the Cardholder. This is known as Dynamic Currency Conversion (DCC). Acquirers must provide field 126.19 - Dynamic Currency Conversion Indicator in all non-ATM, authorization, and full-financial original transactions when the Merchant performs currency conversion at the point of sale. This field contains a value to indicate that the Merchant performed DCC. VEAS logs this field but does not send it to Issuers.

For a description of the Multicurrency Service, refer to the *Visa Europe Technical Service Descriptions*.

## 5.8 Addition to the Message Tracking Table

The DMSA Message Tracking Table (MTT) uses the following fields to match requests and responses and to identify repeat or duplicate requests:

- Field 32 - Acquiring Institution Identification Code
- Field 37 - Retrieval Reference Number
- Field 41 - Card Acceptor Terminal Identification
- Field 42 - Card Acceptor Identification Code
- Field 63.1 - Network Identification Code

DMSA can also use other message fields, such as field 7 - Transmission Date and Time and field 11 - System Trace Audit Number, to link messages, although the system does not retain them in the MTT. The MTT retains a transaction's key field information until the Issuer or STIP sends a response to that transaction. Field 62.2 - Transaction Identifier (TID) and field 90 - Original Data Elements are also key message matching elements.

Acquirers must exercise caution if reusing field 37 values when submitting Authorization Requests. See Section 6.13, *Assured Transaction Response tracking*, for further information. Certain Card type transactions require that the MTT not restore values from certain fields when those values differ between the request and the response, for instance, when the amount in field 4 in the response to certain private-label requests is different from the amount in field 4 in its corresponding original request.

For DMSA-acquired SMS transactions, SMS assigns reject code 0514 if it cannot match the response message in the MTT.

## 5.9 Determination of message destination

Visa Europe assumes responsibility for routing a request to its proper destination. Acquirers do not have to determine the destination of their authorization or financial requests. Acquirers cannot maintain their own files that relate Card numbers to Issuers. VEAS contains current records in what are called account range routing tables. DMSA Acquirers must use Visa-supplied account range routing tables for ATM Transactions. DMSA Acquirers can at their discretion use Visa-supplied account range routing tables for POS transactions.

DMSA selects the message destination based on the information in one or more of the following fields:

- Header Field 5 - Destination Station ID
- Field 2 - Primary Account Number
- Field 100 - Receiving Institution Identification Code
- Field 102 - Account Identification 1
- Field 103 - Account Identification 2
- Field 121 - Issuing Institution Identification Code

DMSA also uses the Issuer's profile from the system tables. The Issuer's profile includes the BIN Control Record (BCR) and the Processing Centre Record (PCR), the Issuer's applicable Account Number ranges, and the Issuer's country code.

DMSA uses field 2 or, if there is a non-standard Account Number, field 121 to determine the destination of Card authorization messages.

Issuers designate which of their Processing Centres should receive the requests. The Issuer associates each Issuer BIN (a range of Card numbers for a specific Card program, such as Visa Classic) with a specific Processing Centre. Optionally, Issuers can control which Processing Centre receives requests for their Cardholders by designating multiple Processing Centres and specifying the types of transactions that should be routed to each Processing Centre.

Visa Europe provides routing services that enable Issuers and Acquirers to specify alternate routing for transactions with specified characteristics. For instance, POS transactions can be routed differently from ATM Transactions; PIN transactions can be routed differently from no-PIN transactions; and DMSC and SMS Exception Transactions can be routed differently from authorizations and financial transactions.

For detailed information about routing options and about routing services offered by Visa Europe, refer to the *Visa Europe Technical Service Descriptions*.

If the destination is a system or a network outside of the Visa Europe System, DMSA has connections, or gateways, to outside systems and networks. VEAS uses Gateway Services to reformat the message, if necessary, and to deliver it to the other system or network through these gateways.

Gateway Services then returns messages to the Member using the same Visa Europe System connection point. For information about available gateways and Authorization Gateway Services, contact Visa Europe Customer Support.

## 5.10 Problems with response code 15 'No such Issuer'

When field 39 - Response Code is returned with the value 15 (No such Issuer), the cause often relates to account range changes. The following are common causes.

### 5.10.1 Routing tables not loaded by Acquirer

One of the most common queries from Issuers is that their Cardholders are unable to perform ATM Transactions whereas POS transactions are successful.

Response code 15 usually indicates that an inactive BIN or inactive Card has been detected during the authorization process. An example of an inactive BIN could be other payment system cards, such as Diners Club or American Express, being incorrectly routed to Visa.

### 5.10.2 Card issued in an inactive range

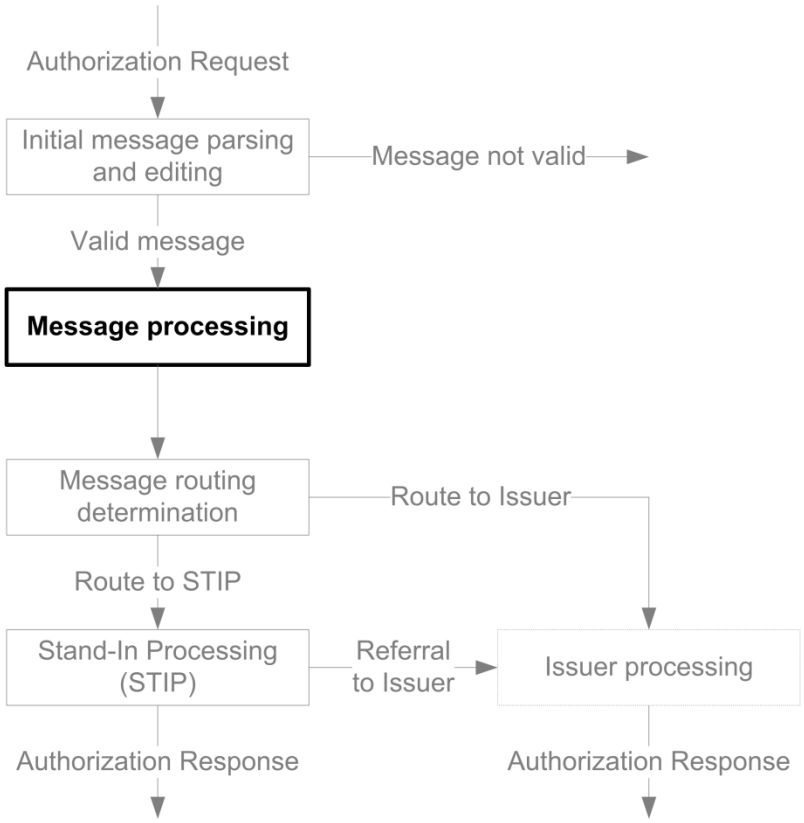
It is the Member's responsibility to ensure that Cards issued to Cardholders correspond to the active account ranges that they submit to Visa. If a Card is issued in an inactive range, Visa will return response code 15, and the Cardholder will not be able to use their Card.

# 6 Message processing

## 6.1 Where message processing fits into the overall DMSA process

Figure 16 illustrates where message processing fits into the overall DMSA process.

**Figure 16: Message processing**




## 6.2 BIN blocking

Issuers can completely block an Issuer BIN by setting the default response code to 57 for all MCGs. If a BIN is blocked in this way, the transaction is not processed by STIP and an advice is not created. The Acquirer receives the response code 57 (decline), and the Issuer receives nothing.

Issuers can also block certain transaction types by blocking their related MCGs using response code 57. In addition to using the default response code 57 to block the entire BIN, Issuers can block an Issuer BIN for domestic cash transactions, for international cash transactions, or for both. If the Issuer blocks the BIN for cash transactions, DMSA declines them with response code 57.

**Note** BIN blocking is subject to applicable local law and the *Visa Europe Operating Regulations*.

### 6.2.1 Country restrictions

- All countries
- Only in the country of issuance

- Only in a selected list of countries
- In all countries except a selected list of countries

Issuers specify country restrictions at the BIN level. Issuers identify Issuer and Card acceptor country codes, as well as the Card type.

If VEAS does not permit the transaction, it declines it with response code 62 - (restricted Card).

### 6.2.2 Risky countries

Issuers can identify up to 20 countries as high risk in the BIN-level Risky Countries table. Issuers can specify that requests originating in risky Acquirer countries be immediately routed to the Issuers when they are available, bypassing Issuer-specified limits and mandatory minimum limits.

If Issuers are unavailable, they can have STIP either respond immediately with predefined response codes (decline) or continue processing according to the Issuers' normal STIP processing parameters.

The available risky country response codes are A (approval) and D (decline). VEAS translates these response codes to 00 and 05 respectively, before it forwards the response to the Acquirer.

VEAS checks the Country Exclusion table before checking the Risky Countries table. If a country is listed in both, the country exclusion processing takes precedence.

**Note** For transactions with countries listed in the Country Exclusion table, VEAS responds with response code 62 (restricted Card) depending on Issuer specifications.

### 6.2.3 Country restriction exception rule

For e-commerce transactions with Merchant Category Code 9701 in field 18, a USD 1.00 status check overrides the country exclusion check so Card verification can be performed prior to issuing a Cardholder certificate. The Certificate Authority, for instance, VeriSign, issues and controls Cardholder certificates.

### 6.2.4 Country-to-Country embargo

DMSA allows Issuers to block transactions originating in or between embargoed countries, for instance, between Acquirers in country A and Issuers in country B. VEAS maintains a Country-To-Country table that allows DMSA Issuers to control purchase and cash transactions between countries using country-specific and BIN-based parameters. Issuers use the table predominately, however, to list countries in which they restrict or prohibit Card usage, for instance, between country A Acquirers and country B Issuers. Only Visa updates the Country-to-Country table.

Issuers set the following parameters to establish a DMSA country-to-country block:

- Issuer and Acquirer country codes
- Card type, for instance, Visa Card
- Card program, for instance, Classic or Platinum
- Whether to block purchase transactions, cash transactions, or both

- Whether Cards are valid in all countries, valid only in the issuing country, valid in countries identified in the table for the BIN, or invalid in countries identified in the table for the BIN
- Whether to exempt the BIN from mandatory limits
- Whether always to route the transaction to the Issuer if available
- Whether STIP should override an Approval Response code (00) with an Issuer-defined response code
- Whether STIP should bypass the $150 rule (see Chapter 8, *Stand-in processing (STIP)*, for information about the $150 rule)

When checking the table, DMSA determines if a country is embargoed and if it is, whether the embargo includes cash transactions, POS transactions, or both. When DMSA finds a match, it inserts response code 62 (restricted Card) in field 39 and STIP declines the transaction.

Issuers can establish country-to-country embargo settings for POS transactions. (Settings for cash transactions are not permitted). DMSA controls country-to-country embargoes.

## 6.3 Random selection factor

For increased risk protection, the Issuer can designate that a percentage of transactions be randomly selected for extra processing. The system uses this percentage (0-30 percent), called a random selection factor, to select transactions for a higher level of processing.

Issuers can specify separate random selection percentages for below-advice-limit and between-limit transactions, respectively, to obtain a sampling of transactions for processing at the higher level. VEAS treats randomly selected below-advice-limit transactions as between-limit transactions, and treats between-limit transactions as above-Issuer-limit transactions. Consequently, activity checking can occur for some transactions that would not otherwise be checked, and routing can occur for some transactions that would otherwise be processed in STIP.

Random selection processing reduces fraud exposure by reducing the chance of predicting STIP authorizations.

## 6.4 Risk level and limits determination

The following factors determine which transactions VEAS sends to stand-in processing (STIP) (this includes services performed in-flight which may send an Authorization Request to STIP):

- Issuer-specified activity limits at the Merchant Category Group (MCG) and totals levels
- Mandatory minimum activity limits at the MCG and totals levels
- Issuer-specified Issuer limits at the MCG level
- Mandatory minimum Issuer limits at the MCG level
- Optional override for mandatory minimum limits
- Transaction jurisdiction (domestic or international)
- Issuer region
- Issuer processing status (available or unavailable)

- CVV
- VSDC
- PIN Verification Service
- Real Time Scoring (RTS)
- Visa Europe Payment Stop Service (VEPSS)
- Visa Risk Options
- ATM/POS Balance services
- Visa product decline options
- V PAY options
- Token/Host Card Emulation options
- Visa Processing Controls

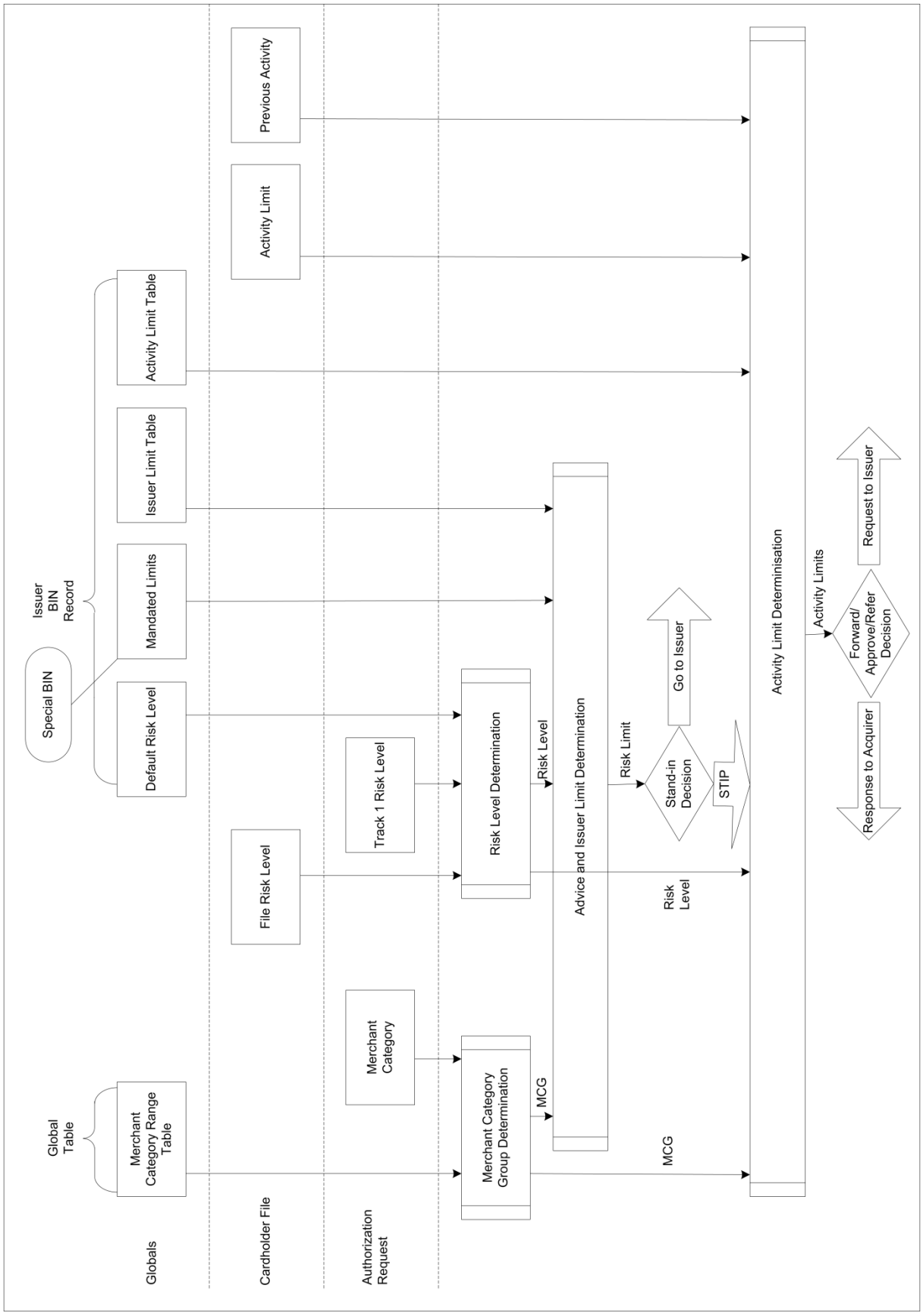
The following factors are involved in STIP performing activity checking and accumulation:

- Selecting risk-level limits and account-level activity limits and determining account listing status, such as VIP (Very Important Person)
- Applying advice limits if appropriate
- Applying between-limits activity checking if appropriate
- Applying random selection factors if appropriate

**Note** VEAS does not apply mandatory minimum Issuer or activity limits to debit or Prepaid Card transactions.

Figure 17 illustrates the switching and STIP processes and the relationship among their applicable elements.

**Figure 17: Switch and STIP processing elements**



**Note** Issuer participation in STIP is mandatory. If the Issuer is unavailable for a transaction, STIP processes it and responds to the transaction with the highest priority response code. Visa Issuers must also participate in Assured Transaction Response (ATR).

## 6.5 Limits overview

Limits are thresholds established by the Issuer or by Visa. DMSA examines every authorization transaction and uses limits to determine whether to route the transaction to STIP or to the Issuer. DMSA also uses limits to determine how transactions are processed within STIP.

There are two basic limits: Issuer limits and activity limits. Both limits are established by the Issuer, with assistance from Visa Europe Customer Support. The limits and their values, along with other processing parameters, are stored in the VEAS system tables.

**Note** Amounts used in DMSA and STIP processing are expressed in USD.

### 6.5.1 Mandatory minimum (MM) limit

For some transactions, VEAS overrides an Issuer-specified Issuer limit or activity limit with a Visa-mandated limit called a mandatory minimum (MM) limit, to facilitate a higher level of Cardholder and Merchant service.

### 6.5.2 Issuer limit

An Issuer limit is an amount that determines whether DMSA routes a transaction to the Issuer Processor or to STIP for an approval, decline, or referral decision. DMSA routes transactions with amounts equal to or greater than the Issuer limit to Issuer Processors for authorization decisions. DMSA routes transactions with amounts less than the Issuer limit to STIP for processing. When the Issuer is not available, STIP also processes transactions with amounts above the Issuer limit.

**Note** Certain rules for specific Card programs can override the Issuer limit.

Issuers specify separate Issuer limits for all MCGs, including Other Purchase and Other Cash.

Table 15 summarises how VEAS applies Issuer-specified or Visa-mandated Issuer limits.

**Table 15: Issuer limit processing decision summary**

| Issuer limit processing decision summary | | | |
|---|---|---|---|
| **Transaction type** | **Issuer limit decision** | | **Exception** |
| | **Use the higher amount of the Issuer limit or Visa mandatory minimum limit** | **Use the lower amount of the Issuer limit or Visa mandatory minimum limit** | |
| T&E, which includes Travel, Lodging, Auto Rental, Restaurant (if the region defines Restaurant as a T&E Transaction) | Yes | No | n/a |

| Issuer limit processing decision summary | | | |
|---|---|---|---|
| **Transaction type** | **Issuer limit decision** | | **Exception** |
| | **Use the higher amount of the Issuer limit or Visa mandatory minimum limit** | **Use the lower amount of the Issuer limit or Visa mandatory minimum limit** | |
| Mail order/telephone order (MOTO) and e-commerce | No | Yes | Based on Member profile parameter, VEAS can bypass PCAS and route all International Transactions directly to the Issuer. |
| Purchase and Cash | Yes | No | n/a |

### 6.5.3 Zero Issuer limits

Issuers can establish zero Issuer limits to have DMSA always forward all applicable transactions to the Issuer, when the Issuer is available. DMSA overrides zero limits and sends transactions to STIP when the following conditions apply:

- Issuer-unavailable conditions
- Timed-out requests
- Issuer-available conditions, but a CVV mismatch triggers an 'all-respond' result

### 6.5.4 Issuer limit exception rules

Issuers can establish Issuer limit exception rules for the following transactions:

**International**: If the Issuer wants to receive all International Transactions, DMSA resets the Issuer limit to zero.

**Key-entered**: If the transaction is not an Account Verification or address verification request, and the Issuer wants to receive all key-entered transactions, DMSA resets the Issuer limit to zero.

### 6.5.5 Mandatory minimum Issuer limits

Issuers in Visa Europe must use MM Issuer limits. Each Visa Inc. region determines whether their issuers must use them.

**Note** These limits only apply to credit products, and only to those credit products that have not opted out. They do not apply to debit products.

For some Visa Card transactions, VEAS overrides an Issuer-specified Issuer limit with Visa MM Issuer limits to facilitate a higher level of Cardholder and Merchant service.

MM Issuer limits apply to the following transactions:

**T&E**: The Issuer can also specify limits for these transactions, and DMSA uses the greater of the two limits.

**e-commerce**: DMSA uses the lower of the mandated or Issuer-specified Issuer limit. DMSA forces the advice limit to zero.

**MOTO**: DMSA routes transactions below that threshold amount to STIP for the approval or decline decision. US-region Issuers must specify that all MOTO transactions be forwarded to them. (The Issuer-available limit is zero.)

When MM Issuer limits apply to low-risk T&E Transactions, VEAS uses the greater value between any Issuer-supplied Issuer limit and the applicable Visa MM Issuer limit. For high-risk transactions, such as MOTO transactions, VEAS uses the lower of the Issuer-supplied Issuer limit and the applicable Visa MM Issuer limit. For all other purchase or Cash Disbursement transactions, VEAS uses the greater of any Issuer-supplied Issuer limit and the applicable Visa MM Issuer limit.

See Appendix C, *Visa Mandatory Minimum Limits*.

### 6.5.6 Advice limit

An advice limit is a Transaction Amount that determines whether STIP performs optional functions when processing transactions below the Issuer limit. Issuers can specify only one advice limit for a BIN. The advice limit is zero for Other Cash, ATM, and Quasi-Cash MCGs. An advice limit can be equal to, or less than, any MCG Issuer limit; advice limits greater than the Issuer limit result in the system choosing the Issuer limit. Issuers do not establish a separate advice limit for when the Processing Centre of the Issuer is available and for when it is unavailable.

Advice limits control whether or not DMSA performs the activity check for the transaction during STIP. The advice limit also controls whether the system creates an advice for the Issuer when STIP approves the transaction.

#### 6.5.6.1 Advice limit exception rules

DMSA changes the advice limit to zero if the Issuer BIN indicates that DMSA is to force-route all MOTO/e-commerce transactions to the Issuer.

The advice limit is zero if the region has mandated a zero Issuer limit for MOTO/ e-commerce transactions.

### 6.5.7 Activity limit

An activity limit is the combination of a Transaction Amount plus the number of times a Card can be used during a given period. Table 16 summarises how STIP applies Issuer-specified or Visa-mandated activity limits.

**Table 16: Activity limit processing decision summary**

| Activity limit processing decision summary | | | |
|---|---|---|---|
| **Transaction type** | **Activity limits decision** | | **Exception** |
| | **Use the higher amount of the Issuer-specified activity limit or Visa mandatory minimum activity limit** | **Use the lower amount of the Issuer-specified activity limit or Visa mandatory minimum activity limit** | |
| T&E, which includes Travel, Lodging, Auto Rental, Restaurant (if the region defines Restaurant as a T&E Transaction) | Yes | No | Codes in the CDB or Exception File limits may override the applicable activity limits. |
| MOTO | Yes | No | |
| Purchase and Cash | Yes | No | |

Issuers specify activity limits to control accumulated Cardholder spending. Issuers can specify activity limits separately for Issuer-available conditions and for Issuer-unavailable conditions.

**Note** DMSA does not check activity and does not update the Activity File if the Transaction Amount is below the Issuer-specified advice limit. (SMS performs activity checking only if the Issuer has specified a value other than zero for the Issuer BIN's activity count.)

Issuers specify activity limits for the following categories of Cardholder spending:

- 1-day count

  The number of times a Card can be used in one day. The one-day count can be any value between zero and 250.

- 1-day amount

  The maximum amount allowed for transactions in one day. The one-day amount can be any USD amount between zero and USD 65,500.

Activity limit default values are 250 (count) and USD 65,500 (amount). For T&E Transactions, using the default values prevents DMSA from checking activity. Also, for T&E Transactions, any applicable mandatory minimum limits take precedence over default values, and DMSA checks activity.

For non-T&E Transactions, mandatory minimum limits do not take precedence over default values, and DMSA checks activity even if default values are being used for limits.

Table 17 shows the relationships of the Issuer-available and Issuer-unavailable activity limits at the BIN level.

**Table 17: Issuer specification requirements for BIN-level Issuer and activity limits**

| Issuer specification requirements for BIN-level Issuer and activity limits | | | | | | | |
|---|---|---|---|---|---|---|---|
| MCG number | MCG name | Issuer available | | | Issuer unavailable | | Pass Either, Pass Both, or Pass Total (see notes after table.) |
| | | Issuer limit | Activity limits | | Activity limits | | |
| | | | 1-Day Amount | 1-Day Count | 1-Day Amount | 1-Day Count | |
| 1 | Airline | Required | Optional | Optional | Optional | Optional | Pass Either |
| 2 | Lodging | Required | Optional | Optional | Optional | Optional | Pass Either |
| 3 | Rental Car | Required | Optional | Optional | Optional | Optional | Pass Either |
| 4 | Restaurant | Required | Optional | Optional | Optional | Optional | Pass Either |
| 11 | Medical | Required | n/a[1] | n/a | n/a | n/a | Pass Totals |
| 5 | MOTO | Required | Optional | Optional | Optional | Optional | Pass Both |
| 6 | Risky Purchase | Required | Optional | Optional | Optional | Optional | Pass Both |
| 7 | Other Purchase | Required | n/a | n/a | n/a | n/a | Pass Totals |
| 7 | Total Purchase | n/a | Required | Required | Required | Required | n/a |
| 9 | ATM Cash | Required | Optional | Optional | Optional | Optional | Pass Both |
| 10 | Quasi-Cash | Required | n/a | n/a | n/a | n/a | Pass Totals |
| 8 | Other Cash | Required | n/a | n/a | n/a | n/a | Pass Totals |
| 8 | Total Cash | n/a | Required | Required | Required | Required | n/a |

n/a - These limits cannot be specified.

### 6.5.7.1 Issuer specification requirements for BIN-level Issuer and activity limits table

Note the following:

- Issuers specify Issuer limits and activity limits only for the first nine categories, that is, category indicators 1 through 9.
- Medical is separately defined as MCG 11, but it uses its own Issuer limit if specified. For activity checking, the activity limit for MCG 07, Other Purchase, is used.
- Quasi-cash is separately defined as MCG 10, but it uses its own Issuer limit if specified. If no Issuer limit is specified, it uses the Issuer limit of MCG 08. For activity checking, the activity limit for MCG 08, Other Cash, is used.
- MCG 07 contains activity limits for Total Purchase and contains Issuer limits for Other Purchase. Issuers cannot specify activity limits for Other Purchase, nor can they specify Issuer limits for Total Purchase.

- MCG 08 contains activity limits for Total Cash and contains Issuer limits for Other Cash. Issuers cannot specify activity limits for Other Cash, nor can they specify Issuer limits for Total Cash.
- The term Other Purchase describes the category of individual Non-Cash transactions that do not meet the requirements for the other POS MCGs. The terms Total Purchase and Total Cash describe the sum of all Purchase or Cash transactions in their respective overall categories (including Other Purchase or Other Cash transactions) that occur within a given period of time.
- **Pass either** Merchant Category Groups: If the Issuer specifies an activity limit or if an MM activity limit applies, a transaction passes activity checking if it passes the activity check at either the MCG level or at the Totals level, that is, a transaction that fails activity checking at the MCG level but passes at the Totals level would pass activity checking. Additionally, a transaction that fails activity checking at the Totals level and passes at the MCG level would also pass activity checking.
- **Pass both** Merchant Category Groups: Transactions fail activity checking if they fail any of the checks, that is, when MCG-level activity limits do not apply (MM limits do not apply and the Issuer did not specify activity limits for this MCG), a transaction must pass Totals activity checking. If MCG-level activity limits apply, the transaction must pass both the MCG-level and Totals-level activity checking to be approved.
- **Pass Totals** Merchant Category Groups: Transactions must pass the Totals activity check to be approved.

Issuers can specify activity limits for:

- Individual accounts in the Cardholder Database

  See Appendix A, *Cardholder Database and Advice Files*, for information about the Cardholder Database.
- Separate activity limits for each Cardholder risk level in the BIN

DMSA uses the Issuer-established Total Purchase and Total Cash activity limits if the Issuer does not define activity limits at the MCG level or at the Merchant category level.

#### 6.5.7.2 Visa minimum T&E activity limits

Visa has established MM activity limits for transactions involving specific travel and entertainment (T&E) Merchant categories. These categories are Commercial Travel, Lodging, and Auto Rental.

When these limits apply to a transaction, DMSA uses the greater of the Issuer-specified activity limit or the applicable MM activity limit according to the jurisdiction (domestic or international) of the transaction.

**Note** These limits only apply to credit products. The Issuer can opt out of these limits if they wish.

#### 6.5.7.3 Visa minimum non-T&E activity limits

DMSA uses the greater of the Issuer-specified activity limits or the applicable MM activity limit. See Appendix C, *Visa Mandatory Minimum Limits,* for the Visa MM activity limits. If Visa does not specify a Visa MM activity limit or if it is zero, then VEAS uses the Issuer-specified activity limit.

#### 6.5.7.4 Choosing Issuer-specified or Visa-mandated limits for routing and STIP

VEAS routes a transaction to the Issuer or to STIP according to whether the Transaction Amount in field 4 exceeds the Issuer-specified Issuer limit threshold amount or, if applicable, the Visa-specified MM Issuer limit.

To determine which of these limits applies, VEAS follows the procedure outlined in Table 18. The table also illustrates how STIP decides between Issuer-specified activity limits (counts and amounts) and Visa-mandatory minimum activity limits to resolve the transaction's effect on the Cardholder's allowable activity limits. A key aspect of the decision process is if one limit's amount is greater (or larger) than the other (less or lower).

**Table 18: Choosing Issuer-specified or Visa-mandated limits**

| Choosing Issuer-specified or Visa-mandated limits | | | | |
|---|---|---|---|---|
| **To determine the following limit** | **For this transaction type** | **Issuer-specified Issuer limit** | **Visa mandatory minimum Issuer limit** | **Use the following limit** |
| **Issuer limit** | T&E | Lower | Higher | Visa mandatory minimum Issuer limit |
| | T&E | Higher | Lower | Issuer-specified Issuer limit |
| | MOTO | Lower | Higher | Issuer-specified Issuer limit |
| | MOTO | Higher | Lower | Visa mandatory minimum Issuer limit |
| | Purchase & Cash | Lower | Higher | Visa mandatory minimum Issuer limit |
| | Purchase & Cash | Higher | Lower | Issuer-specified Issuer limit |
| **Activity limit** | All transactions | Lower | Higher | Visa mandatory minimum activity limit |
| | | Higher | Lower | Issuer-specified activity limit |

### 6.5.8 Cardholder risk levels

Issuers use Cardholder risk levels to tailor authorization routing parameters for Cardholders within a BIN. DMSA processes a transaction assigned to one of the risk levels according to the Issuer limits and the activity limits specified for its respective risk level. Table 19 summarises the four levels.

**Table 19: Cardholder risk levels**

| Cardholder risk levels | | |
|---|---|---|
| **Risk level** | **Applies to** | **Comments** |
| A | Premier or lowest risk accounts | Generous parameters. |

| Cardholder risk levels | | |
|---|---|---|
| **Risk level** | **Applies to** | **Comments** |
| B | Lower or higher risk accounts | Parameters established according to Issuer preference. |
| C | Median risk accounts | DMSA default; established at BIN level. |
| D | Highest or greatest risk accounts | Cardholder account level only; cannot be used as BIN default. Not subject to the mandatory minimum Issuer limits or advice limits. |

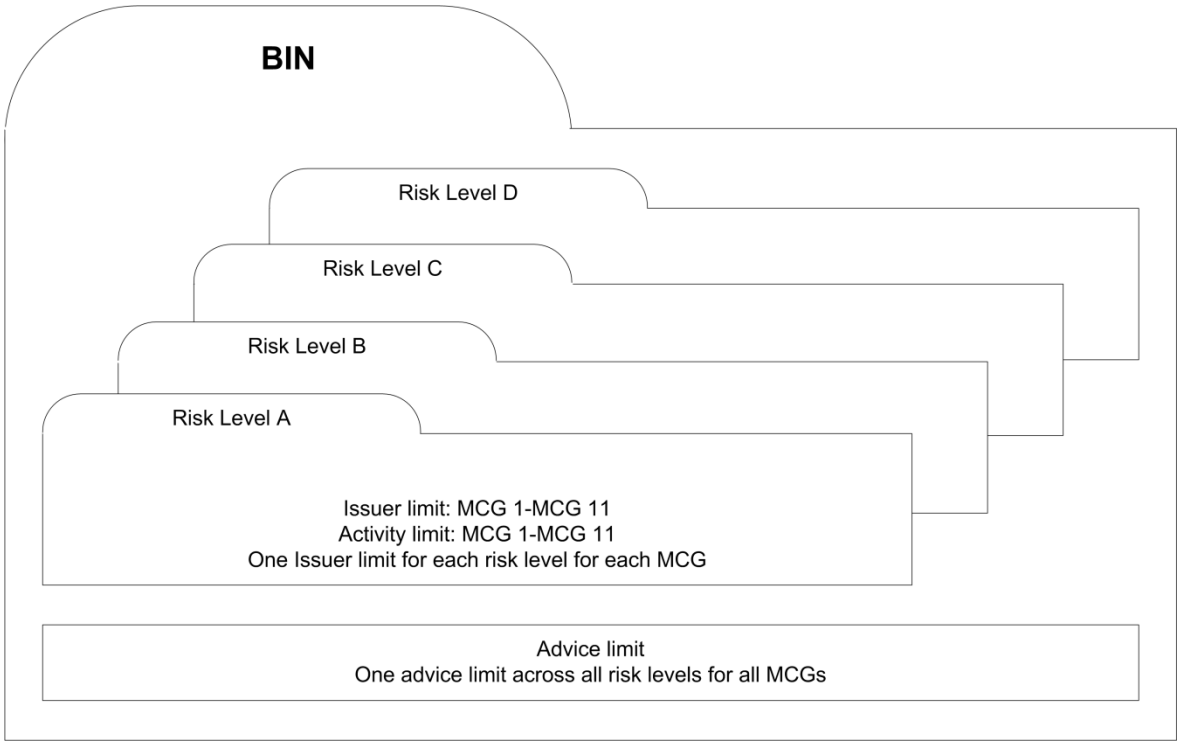
Issuers can establish activity limits at the individual Cardholder level in the risk-level file or in classes of Cardholders by risk level at the BIN level. Activity limits assigned to risk levels are referred to as Cardholder risk-level limits. Processing Centres of Issuers can assign one or more of the following limits to each risk level:

- Activity limits by MCG, which include:
  - Count and amount limits
  - 1-day and 4-day multipliers (see Chapter 8, *Stand-in processing (STIP)* for information about 4-day multipliers)
  - Issuer-available and Issuer-unavailable processing parameters

  **Note** Cardholder risk-level activity limits override any BIN-level 1-day amounts.
- Random selection factors for transactions with amounts that are between established limits
- Advice-creation and activity-checking options for transactions with amounts that are between established limits

Issuers can establish separate sets of Issuer limits and activity limits for each risk level within a BIN. Figure 18 shows the relationship of the Issuer limit and the advice limit settings for Cardholder risk levels.

**Figure 18: Issuer and advice limit settings**




For instance, the Issuer limit for the Restaurant MCG could be USD 200.00 for risk level A and be USD 75.00 for risk level C. These limits would mean that for risk level A Cardholders, DMSA would route all Authorization Requests for the Restaurant MCG of USD 200.00 or more to the Issuer for processing. STIP would process requests under USD 200.00. For risk level C Cardholders, DMSA would route all Authorization Requests for the Restaurant MCG of USD 75.00 and above to the Issuer for processing. STIP would process requests under USD 75.00.

Issuers can override default risk levels by one of two methods:

- Encoding Track 1 in the magnetic stripe of the Card when the Issuer issues the Card

  Visa Europe does not recommend this method because a relatively high percentage of transactions do not contain Track 1 data.
- Adding an account to the risk-level file in the Cardholder Database (CDB)

  Issuers can use this method to optionally override the risk level on the magnetic stripe. See Appendix A, *Cardholder Database and Advice Files*, for information about the CDB.

Although DMSA usually does not retrieve the CDB during routing determination, DMSA retrieves the CDB if the Issuer uses the risk-level file. The order of risk-level selection is:

1. CDB risk level
2. Magnetic stripe (when present)
3. Default risk level for the BIN

Issuers must specify an Issuer limit for each MCG for each risk level if they want to specify more than one risk level. Activity limits specified at the BIN default risk level do not apply to accounts on the non-default risk level.

Issuers establish a single default Issuer limit risk level for the entire BIN; typically risk-level C. Issuers cannot use risk-level D for the BIN default level.

**Note** Some Issuers from Visa Europe have established sets of risk level parameters in advance of busy periods of transaction processing. During those busy periods, they can request Visa Europe to switch from one default risk level to another, thereby alleviating pressure on their own processing system.

## 6.6 Allocation of transaction category

VEAS groups every DMSA authorization into the following three transaction categories:

- Below-advice-limit STIP transactions

  The Transaction Amount is less than the advice limit. For these transactions, DMSA does not perform activity checking or create advices for approved transactions.

- Between-limit STIP transactions

  The Transaction Amount is equal to or greater than the advice limit and less than the Issuer limit. DMSA performs activity checking, advice creation, or both, according to Issuer options.

- Above-Issuer-limit transactions

  The Transaction Amount is equal to or greater than the Issuer limit. The Visa Europe System always routes these transactions to the Issuer.

STIP processes below-advice-limit and between-limit transactions according to other PCAS rules. Figure 19 shows the relationship between these limits.

**Figure 19: Processing with different Issuer and advice limits**

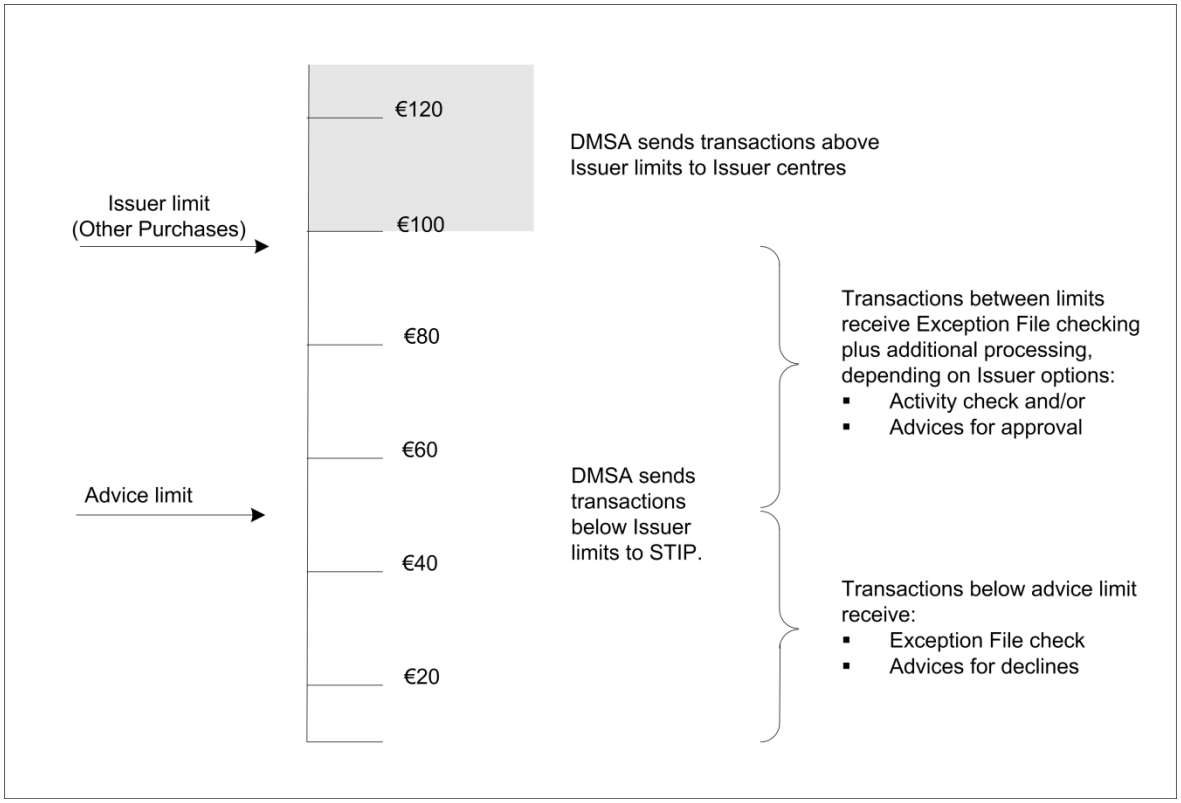



Table 20 shows how STIP determines whether to create advices for non-approved PCAS between-limit transactions.

**Table 20: Advice creation for non-approved PCAS between-limit transactions**

| Advice creation for non-approved PCAS between-limit transactions | |
|---|---|
| **CORE setting** | **STIP decision** |
| Activity Testing On | Selecting YES or NO determines whether STIP is to check activity limits for between-limit transactions. When activity exceeds Issuer-specified activity limits, STIP forwards the Authorization Request to the Issuer for a response. |
| Advice Creation On | For PCAS participants, selecting YES or NO determines whether STIP is to create advices for approved between-limit transactions. STIP creates advices for all non-approved PCAS transactions. |

## 6.7 PIN verification

When VEAS receives a PIN-based Authorization Request for an Issuer that participates in the PIN Verification Service (PVS), the Issuer can choose to have VEAS verify PINs on behalf of the Issuer centre at all times or only when the centre is unavailable.

**Note** PINs are translated in VSDC PIN change or unblock requests, but PIN Verification is not performed. PIN change and unblock requests are valid for UK-Domestic Transactions only.

The Visa Security Module (VSM) verifies PIN validity using Visa PIN Verification Values (PVVs) or Issuer-supplied IBM PIN offsets. DMSA records each incorrect PIN-entry attempt and accumulates the total in the Cardholder Database's Activity File. If the PIN is incorrect or if the PIN is correct but too many unsuccessful PIN-entry attempts have occurred, VEAS forwards the request to STIP for a decline or pick-up response, depending on Issuer specifications.

If Issuers do not use PVS, their one-day amounts for ATM Cash Disbursement requests must be zero, and the default response code used by STIP for those ATM requests must be response code 86 (unable to verify PIN).

For information about the Activity File and about the Cardholder Database, see Appendix A, *Cardholder Database and Advice Files*. For a description of PVS, refer to the *Visa Europe Technical Service Descriptions*. For specific technical specifications for PIN translation and verification, refer to the *Payment Technology Standards Manual*.

## 6.8 Card verification (CVV, iCVV, or dCVV)

VEAS performs Card verification processing on the CVV or iCVV from the track data or from the Chip, depending on whether field 22 - Point-of-Service Entry Mode Code indicates that the magnetic stripe or the Chip was read at the terminal.

If VEAS performs dCVV validation for Issuers that support contactless transactions, it verifies the dCVV in Track 1 or Track 2 of the magnetic stripe using the Application Transaction Counter (ATC), which is also located in Track 1 or Track 2. The dCVV overrides any CVV or iCVV data located in the track. Issuers can choose to have VEAS validate the dCVV in all dCVV-eligible Authorization Requests.

Depending on Issuer specifications, VEAS:

- Validates the CVV, iCVV or dCVV on all requests and forwards the results to the Issuer in the request

- Validates the CVV, iCVV or dCVV on all requests and if the validation fails, responds to the Acquirer using the Issuer's specified response code
- Validates the CVV, iCVV or dCVV in a request only when the Issuer is unavailable and it sends the request to STIP
- Forwards all requests to the Issuer without validating the CVV, iCVV or dCVV

See Section 8.4.3, *Card verification failure - CVV, iCVV, dCVV*, for information about how STIP verifies CVV, iCVV, and dCVV. See also Appendix B.4.1, *CVV and iCVV* and Appendix B.5, *Contactless processing (dCVV)*, for more information.

## 6.9 CVV2 verification

The CVV2 is keyed by the Merchant or the Cardholder. Depending on Issuer specifications, VEAS:

- Validates the CVV2 on all requests and forwards the results to the Issuer in the request
- Forwards all requests to the Issuer without validating the CVV2

If VEAS performs CVV2 validation for the Issuer, it verifies the CVV2 before it passes the Authorization Request to the Issuer or to STIP. Issuers can choose to have VEAS check the CVV2 in all CVV2-eligible Authorization Requests.

For CVV2 verification-only status checks, the amount in field 4 can be zero in requests and their reversals, if:

- Field 3 - Processing Code, positions 1-2, contains 39 (eligibility message), 70 (PIN change/unblock), 72 (PIN unblock or prepaid activation)
- Field 25 - Point-of-Service Condition Code contains 51 (zero amount Account Verification)
- Field 126.10 - CVV2 Authorization Request Data is present

Also, field 4 can contain zero in 0302 file update requests or 9620 fraud advice requests. If the request meets all the verification-only field requirements, and field 4 contains an amount other than zero, STIP ignores the amount and, if the request is successful, responds with a value of 85 (no reason to decline) in field 39.

**Note** If a request contains both a CAVV and a CVV2, CAVV validation takes precedence over CVV2 validation. For further information concerning VEAS processing when both elements are present in a request, refer to the *Visa Europe Technical Service Descriptions*.

See Section 8.4.4, *Card verification failure (Card-not-present) - CVV2*, for information about how STIP verifies CVV2. See also Appendix B.4.2, *CVV2*, for more information.

## 6.10 Account Verification or address verification-only status checks

Account Verification, address verification, or CVV2 verification-only requests can be used for status checks.

The amount in field 4 can be zero in requests and their reversals if:

- Field 3 - Processing Code, positions 1-2, contains 39 (eligibility message), 70 (PIN change/unblock), or 72 (PIN unblock or prepaid activation)

- Field 25 - Point-of-Service Condition Code contains 51 (zero amount Account Verification)
- Any of:
  - Field 52 - PIN Data, and field 53 - Security-Related Control Information are present
  - Field 123 - Verification Data is present
  - Field 126.10 - CVV2 Authorization Request Data is present

Also, field 4 can contain zero in 0302 file update requests. If the request meets all the verification-only field requirements, and field 4 contains an amount other than zero, STIP ignores the amount and, if the request is successful, responds with a response code value of 85 (no reason to decline) in field 39.

For Account Verification, the 0100 Authorization message contains the following:

- Field 4 - Amount, Transaction = 0 (zero)
- Field 25 - POS Condition Code = 51 (Account Verification)

If the Issuer is available, VEAS forwards the request message to the Issuer. The Issuer performs normal transaction verification and returns an appropriate response code. If no negative condition is found and the account is in good standing, the Issuer returns response code 85 in field 39.

If the Issuer is unavailable, VEAS performs normal stand-in processing validation. If no negative condition occurs, VEAS returns response code 85 in field 39.

## 6.11 Verified by Visa verification (CAVV)

If Issuers participating in the Cardholder Authentication Verification Value (CAVV) Verification Service have VEAS perform CAVV validation, VEAS performs the verification after determining Issuer availability. The Visa Security Module (VSM) uses authentication data elements in field 126.9 - CAVV Data and field 126.8 - Transaction ID (XID) (or just field 126.9 if field 126.9, Usage 3 - 3-D Secure CAVV, Revised Format is being used) along with Issuer-supplied keys. (Authentication and Attempt transaction keys may be the same.)

Depending on Issuer option elections for CAVV Authentication transactions, VEAS:

- Performs all CAVV validation on the Issuer's behalf, declines transactions when CAVV validation fails, and forwards status results on transactions that were not declined to the Issuer
- Validates the CAVV using Issuer-supplied keys and passes all results to the Issuer regardless of the outcome
- Forwards the transaction to the Issuer without validating the CAVV

Depending on Issuer option elections for CAVV Attempt transactions, VEAS:

- Validates the CAVV using Issuer-supplied keys and passes the CAVV result for non-declined transactions to the Issuer in the request message
- Validates the CAVV using Issuer-supplied keys and passes all results to the Issuer regardless of the outcome
- Forwards the transaction to the Issuer without validating the CAVV

For Issuers that validate CAVVs, VEAS checks the value in field 44.13 - CAVV Results Code. If the value is 0, which indicates that the CAVV authentication results are invalid, VEAS performs one of the following checks:

- If VEAS has the CAVV keys, and the CAVV results code validated by VEAS is not 0 (indicating that the first three positions of field 126.9 are valid), VEAS replaces the 0 value in field 44.13 with a valid CAVV results code and forwards the response message to the Acquirer
- If VEAS does not have the CAVV keys and VEAS determines that the first three positions of field 126.9 do contain valid values, VEAS replaces the 0 value in field 44.13 with C (CAVV was not validated - Attempt) or D (CAVV was not validated - Authentication) and forwards the response message to the Acquirer
- If VEAS has the CAVV keys, and the CAVV results code validated by VEAS is 0 (indicating that the first three positions of field 126.9 are not valid), VEAS forwards results code 0 in the response message to the Acquirer

CAVV transaction processing rules depend on transaction characteristics and on Issuer-specified STIP processing parameters. If STIP processes a CAVV request and the validation fails, the default response code is 05 (do not honour).

For DMSA, if the Issuer's selected CAVV Attempt or Authentication option in the Customer Online Repository (CORE) is F or V, VEAS forwards the field 44.13 CAVV result code in the request to the Issuer. If the Issuer responds with a result code other than the one it received, VEAS overrides the Issuer's result code with its own before it sends the response to the Acquirer.

See Section 8.4.5, *Verified by Visa failure - CAVV*, for information about how STIP validates CAVV. See also Appendix B.17, *Verified by Visa Service and Electronic Commerce Transactions (CAVV)*, for more information.

## 6.12 VSDC authentication

The VSDC Service supports the Card Authentication feature and the Issuer Authentication feature. Both features are optional and available to Full Data participants (participants that fully participate in the VSDC Service).

The Card Authentication feature validates static and variable data in the request message, such as the Account Number and the Transaction Amount. The request includes a Card-generated Cryptogram and a Triple Data Encryption Standard (TDES) key that is loaded on the Card during personalisation or is produced during a dynamic key-generation session. For Card authentication, Cryptogram version 10 is valid for Visa Integrated Circuit Card Specification (VIS) Card types. Issuers can use Cryptogram version 12 to define their own Cryptogram versions for Card types other than CCD-compliant.

If the Visa Europe System performs the authentication on the Issuer's behalf, it forwards the result to the Issuer in the request. For Full Data Issuers, VEAS also includes the Card authentication reliability indicator in field 60.7 and audit trail data. For further information about which conditions must be met for VEAS to perform the authentication, refer to the *Visa Europe Technical Service Descriptions*.

The Issuer Authentication feature verifies that the response message came from the correct Issuer. If the Issuer supports the feature, either the Visa Europe System or the Issuer generates a Cryptogram (different from the one for Card authentication) that is included in the response to Full Data Acquirers. The Card uses the Cryptogram to determine Issuer authentication.

For further information about VEAS processing of Chip Transactions, refer to the *Visa Europe Technical Service Descriptions*, and to the latest version of the *Visa Smart Debit/Credit System Technical Manual*. Members can contact Visa Europe Customer Support to obtain a copy of this manual.

**Important** Field 55 may contain tags that the receiving Issuer or Acquirer does not recognise, or does not expect. The receiver must ignore such tags, and continue parsing the next tag in field 55.

## 6.13 Assured Transaction Response tracking

The Assured Transaction Response (ATR) function monitors all Authorization Requests forwarded to Issuers to ensure each request receives a timely Authorization Response. There is a default time limit that VEAS allows for European Issuers (five seconds). This value may sometimes be adjusted to meet certain Issuer configurations. Other Visa regions may set different time-out limits.

If an Issuer does not send an Authorization Response to VEAS within the specified time limit, VEAS invokes STIP to determine the approval or decline decision on the Issuer's behalf. If an Issuer sends a response to an Authorization Request after VEAS has diverted the same request to STIP, the STIP-generated decision prevails; VEAS discards the late response from the Issuer.

ATR applies to both DMSA and SMS Issuer Processors. Before VEAS routes the request to the Issuer, it copies the message to the ATR table and sets the timer to monitor how long the message is with the Issuer. If VEAS finds no Issuer-specified timeout values at the PCR or station levels, it uses default timeout values to determine whether the request has been with the Issuer too long without resolution. When the timeout value (whether Issuer-specified or system default) is exceeded, DMSA diverts the message to STIP for the approval or decline decision according to Issuer-specified STIP parameters. DMSA then forwards the response to the Acquirer; DMSA may create an advice for the Issuer, if applicable.

**Note** If an Authorization Request is diverted to STIP because of an ATR time-out, the response generated is determined against Issuer-unavailable parameters.

If the request cannot reach the intended Issuer Processor (for instance, the line is down) and is returned to DMSA before the ATR time runs out, and if the Issuer has another station available, DMSA routes the message to that available station and restarts the timer. If no Issuer stations are available, DMSA forwards the message to STIP.

The ATR function comprises a series of time-limit settings for different Issuer processing conditions.

### 6.13.1 VEAS default timeout values

For non-Visa Europe issuers, if the Issuer does not specify a timeout value, the maximum default timeout value is 60 seconds.

If VEAS intervenes with the default timeout, it forwards the response to the Acquirer with the STIP approval or decline decision but generates no advice for the Issuer.

### 6.13.2 Possible causes of ATR problems

These are the most likely causes of ATR problems.

#### 6.13.2.1 Problem - No response from host

The Member is unavailable, and likely causes are:

- The Member host crashed and the Member was unable to sign off to VEAS
- The connection between the EA Server and the Member's host has failed
- The Member carried out a scheduled shutdown of the host for maintenance and did not sign off to VEAS

#### 6.13.2.2 Problem - ATR - Late response from Issuer host

- There are communications errors on the network
- The Member's host is processing transactions slowly

#### 6.13.2.3 Problem - Discarded messages

- The response from the Member does not match the record in the MTT
- The Member did not retain/return mandatory key fields

#### 6.13.2.4 Problem - Rejected messages

- The response from the Member has an invalid value in one of the fields
- The response from the Member is missing a required field

## 6.14 Repeat or duplicate Authorization Requests

Repeat, or duplicate, Authorization Requests occur when Acquirers send a repeat request message before receiving the 0110 response for the initial request message. Repeat or duplicate messages are identified by a 1 in the last position of the message type designator; for example, 0101. For the purposes of this description, the terms repeat and duplicate are interchangeable.

**Important** VEAS does not permit repeat (duplicate) request messages for ATM Transactions (DMSA and SMS) or POS transactions (SMS)

### 6.14.1 Acquirer processing considerations

If an Acquirer submits an identical Authorization Request (0100/0101) or reversal (0400/0401) within a few seconds of VEAS having already responded to the original, VEAS will treat the message as it would an original request.

**Note** The V.I.P. System, used by authorization processors outside of Visa Europe, has a ten second 'memory' for responded transactions. If V.I.P. receives an identical request and it still has a record of the transaction in memory, it will respond back to the Acquirer immediately with the original response.

If an Acquirer receives a 0110 response after they have timed out the corresponding request in their own authorization system, they should use a 0400 reversal to ensure that the transaction is properly voided.

Acquirers should ensure that their Merchants know to re-swipe the Card when resubmitting an Authorization Request after the previous request has been reversed.

### 6.14.2 Issuer processing considerations

If the Issuer returns a response that does not contain matched MTT fields from the original request, VEAS rejects the Issuer's response (it is assumed to be an unsolicited message). STIP then processes the transaction according to Assured Transaction Response (ATR) rules, if they apply.

Similarly, if VEAS receives a late response from the Issuer, one of the following occurs:

- If received while STIP is already processing the request, then VEAS logs the Issuer's late response to an exception log and discards it
- If received after STIP has responded on the Issuer's behalf, then it treats the response as unmatched and rejects the response as unsolicited

### 6.14.3 Retrying a transaction

If the request times out, and an Acquirer chooses to retry the Authorization Request, the following messages are required:

- For POS transactions: a repeat or a reversal

  For POS transactions destined for SMS Issuers, SMS Issuers receive 0101 repeat messages as message type 0101. However, VEAS converts 0401 messages from DMSA acquirers to 0420 messages before forwarding them to SMS Issuers.

- For ATM Transactions: a reversal followed by a new request

  **Note** The Visa Europe System does not permit repeats for ATM Transactions or SMS POS transactions.

  For ATM Transactions destined for SMS Issuers that participate in the ATM Format Conversion Service (which is mandatory in Visa Europe), Visa Europe converts 0101 repeat messages from DMSA Acquirers to 0200 messages and converts 0401 messages to 0420 messages before forwarding them to SMS Issuers.

  **Note** DMSA Acquirers can identify duplicate responses received from SMS Issuers by checking the value in field 38 - Authorization Identification Response. This value will be the same value in a duplicate response as that in the original response.

  **Important** SMS Issuers processing POS transactions must be prepared to repeat Authorization Request messages. If a DMSA Acquirer sends a 0101 POS request message after an original no longer contained in the MTT, the SMS Issuer will receive that 0101 request.

Visa recommends limiting repeat message submissions to three per request. For information about how VEAS processes undeliverable requests, see Section 4.5, *Undeliverable messages*.

## 6.15 Original Credits for online gambling prohibited by law

VEAS does not allow online gambling OCTs destined to recipient Issuers in countries where online gambling is prohibited by law. VEAS declines the transaction with response code 93 - (transaction cannot be completed - violation of law).

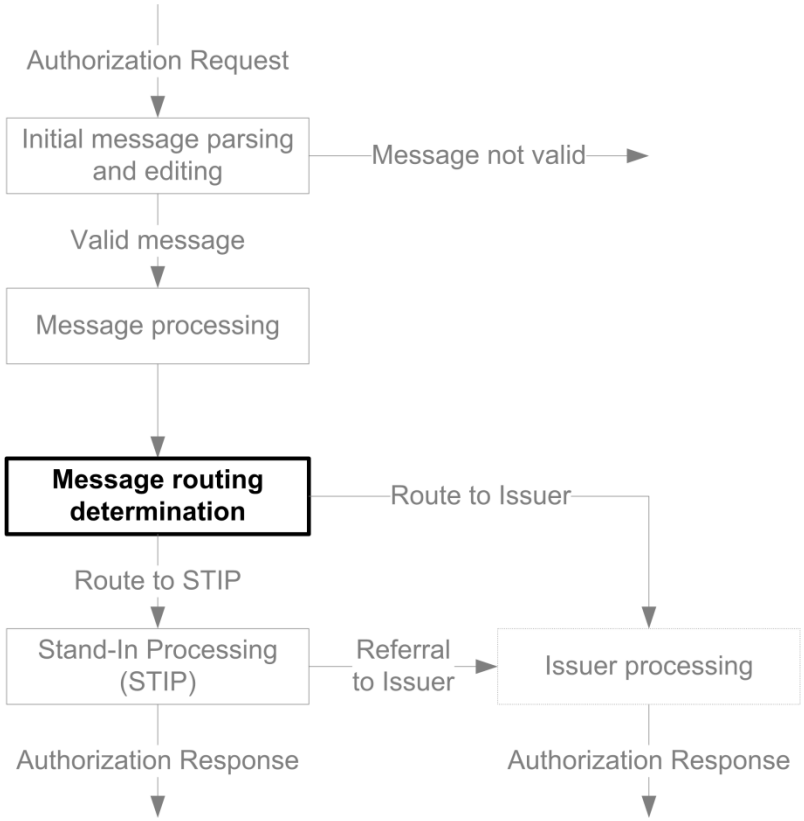
# 7 Message routing

Deciding whether to send an Authorization Request or reversal to the Issuer or to STIP depends on the transaction's characteristics and on PCAS processing rules. It also depends on the Issuer's operating status, that is, whether the Issuer is available or unavailable. Section 6.4, *Risk level and limits determination*, describes these subjects in detail.

## 7.1 Where message routing fits into the overall DMSA process

Figure 20 illustrates where message routing fits into the overall DMSA process.

**Figure 20: Message routing**




## 7.2 Issuer available and Issuer unavailable modes

A Processor is considered available if it has at least one station signed on to the Visa Europe System. When a station is signed on, it is in normal operating mode and can process:

- Outgoing authorization and reversal requests and responses
- Incoming authorization and reversal requests and responses
- Outgoing file maintenance requests and inquiries and their responses
- Outgoing and incoming network management messages
- Incoming administrative messages

The Processor is considered unavailable if:

- The Processor is not linked to the Visa Europe System (or the only link is through the Auto-Telex System)
- The Processor is signed off (or down) or the communications link is down
- The queue of messages awaiting delivery to the Processor exceeds a system-defined limit
- The Processor has failed to respond within the ATR time-out period

See Section 6.4, *Risk level and limits determination*, for more information about Issuer limits and about Issuer-available and Issuer-unavailable conditions.

## 7.3 Suppress Inquiry (SI) mode

Suppress Inquiry (SI) mode allows Processors to control input and output message processing during heavy traffic periods. When the centre assigns SI mode to a station, DMSA blocks all routine incoming Authorization Requests and reversal requests from entering that station. This mode reduces the volume of requests arriving at the station, enabling the station to concentrate on processing outgoing requests.

When a Processor is in SI mode, DMSA cycles through all of the Processor's stations until it finds an available station not in SI mode that can receive the requests that DMSA is trying to deliver. If all of the stations at a centre are in SI mode, PCAS diverts transactions to STIP using Issuer-unavailable limits. STIP forward-refers eligible transactions, see Section 7.3.2, *SI Mode penetration*. If the transaction is not forward-referable or if the Issuer is unavailable, STIP processes the request using the appropriate limits and sends the response to the Acquirer.

### 7.3.1 Signing on and off SI mode

A centre enters and exits SI mode by using 0800 network management messages. In field 70 - Network Management Information Code, the sign-on code is **062** and the sign-off code is **063**. Refer to the field 70 description in *DMSA Technical Specifications* for more information.

VICs can place a centre in SI mode when the centre has processing problems, for instance, an excessive number of time-outs. The VIC tries to notify the centre beforehand, but if a centre cannot be reached, the VIC invokes SI mode while continuing its attempts to notify the centre.

### 7.3.2 SI Mode penetration

Even though a station is in SI mode, STIP can still forward a request to the station under certain conditions:

- The Cardholder-available activity limits are exceeded
- The account is listed in the Exception File with a non-approval code other than a decline
- The transaction failed the CVV/iCVV check
- The Card product is Visa Infinite, Visa Signature, or Visa Signature Preferred
- The transaction is a large US federal tax payment
- The transaction is acquired in a risky country as defined by the Issuer
- The transaction is a UK - domestic Address Verification Service (AVS) transaction

- The transaction is one of the following ATM/MOTO/Electronic Commerce Transactions regardless of activity limits:
  - ATM Balance Inquiries
  - ATM Transactions in which field 52 - Personal Identification Number (PIN) Data is present, and field 53 - Security-Related Control Information, positions 1 and 2, does not contain 20
  - ATM Transactions in which field 52 is present, subfield 53.1 contains 20, and the Issuer has selected the PIN translation option but no PIN Verification Service (PVS) algorithm has been specified
  - The Member opts to decline key-entered transactions
  - Recurring payment transactions

When the Visa Europe System force-routes a transaction, STIP invokes mandated STIP Decline Responses when it encounters Issuer-unavailable conditions. See Chapter 8, *Stand-in processing (STIP),* for information about force-routed transactions.

When this situation occurs, the request is said to "penetrate" SI mode and this situation is often called an "SI penetration." This feature is useful when STIP finds a high priority condition that warrants the attention of the Processor of the Issuer.

The forwarded request includes a STIP code indicating the forwarding reason. If the centre does not return a response or if the Issuer centre is not available, STIP processes the transaction using the Issuer's unavailable limits.

## 7.4 Routing to STIP

DMSA processing uses the Positive Cardholder Authorization Service (PCAS) to establish limits to use for routing and STIP. DMSA uses PCAS-established limits, such as Issuer, advice, and activity limits, to route transactions to the Issuer or to STIP using Issuer limit amounts.

### 7.4.1 Overview of factors that determine routing to STIP

Stand-in processing (STIP) makes authorization decisions to approve or decline a transaction on the Issuer's behalf.

DMSA routes transactions to STIP when:

- The Issuer is unavailable because either of the following conditions applies:
  - No Issuer stations are signed on, all of the Issuer's stations are temporarily unavailable, or the lines to the Issuer are down.
  - The message was sent to an Issuer but no response was received within the time limit.
- The Issuer is available and one of the following conditions applies:
  - The Transaction Amount is below the Issuer-specified Issuer limit, or, if applicable, below the mandatory minimum Issuer limit.
  - The Issuer subscribes to certain Visa Europe services, such as Card Verification Value (CVV) Service, Card Verification Value 2 (CVV2) Service, Cardholder Authentication Verification Value (CAVV) Verification Service, Dynamic Card Verification Value

(dCVV) Service, PIN Verification Service (PVS), or Address Verification Service (AVS), and the Issuer wants STIP to process the transaction depending on the results.

- The Issuer is in Suppress Inquiry (SI) mode, and the transaction type is not one that is allowed to penetrate SI mode.
- The transaction is below the Issuer-specified Issuer limit, and the Issuer is available but has chosen not to receive forward referrals from STIP. However, in this case, STIP processes the transaction as if the Issuer is unavailable.

### 7.4.2 Rules for routing to STIP

DMSA routes below-Issuer-limit transactions to STIP.

Table 21 lists exception rules for the STIP or switch decisions by transaction type.

**Table 21: STIP/switch decision rules**

| STIP/switch decision rules | | | |
|---|---|---|---|
| **Transaction type or condition** | **Always switch to available Issuers** | **Processed in STIP** | **Comments** |
| Transactions with amounts below the advice limit | | X | n/a |
| Transactions with amounts above the Issuer limit | X | | n/a |
| Transactions where Issuer performs PIN, CVV, iCVV, or CAVV verification | X | | n/a |
| Transactions where the Visa Europe System performs PIN, CVV, iCVV, or CAVV verification | | X | n/a |
| MOTO | X | | DMSA always switches MOTO transactions to available Issuers in the US region. |
| ATM balance inquiry | X | | Ineligible for STIP. |
| Automated dispensing machine (ADM) | X | | n/a |
| Transactions involving risky countries | X | | The Risky Countries table indicates force-to-Issuer.<br>**Note** VEAS responds to transactions involving excluded countries with response code 62 depending on Issuer specifications and regardless of Issuer availability. |
| Authorization Requests for Merchandise and Services (field 18 Merchant Category Code 6012) | X | | n/a |

| STIP/switch decision rules | | | |
|---|---|---|---|
| **Transaction type or condition** | **Always switch to available Issuers** | **Processed in STIP** | **Comments** |
| One unit of currency | X | | Transaction uses one unit of currency (USD 1.00 authorization) and is not an ATM withdrawal (based on the value in field 18). |
| Private-label transactions | X | | n/a |
| Account Verification Requests | X | | Transaction for a zero amount and with POS condition code of 51. |
| Certain Visa Electron Transactions | | | If a PIN is present, the transaction is not ATM (field 18 does not contain 6011), VEAS is not verifying the PIN, and any of the following options are not set to On:<br>■ Decline all non-Domestic Transactions<br>■ Decline POS transactions with PINs in STIP<br>■ Decline all POS transactions with PINs<br>If the Issuer BIN has any of the following Visa Electron options selected:<br>■ Decline Card-not-present transactions in STIP<br>■ Decline POS transactions with PINs in STIP<br>■ Decline POS transactions without PINs in STIP |
| Recurring payment transactions | X | | If the Issuer is unavailable, STIP processes the transaction according to Issuer parameters. |
| PIN change or unblock transactions (Visa Smart Debit/Credit [VSDC] PIN Management Service; UK-Domestic Transactions only) | X | | If the Issuer is unavailable or times out, STIP responds with response code 91. |
| POS balance inquiry (standalone) | X | | Ineligible for STIP. |
| V PAY | X | | |

| STIP/switch decision rules | | | |
|---|---|---|---|
| **Transaction type or condition** | **Always switch to available Issuers** | **Processed in STIP** | **Comments** |
| VSDC: Issuer Application Data (IAD) length limit exceeded for VIS or CCD Card types | X | | VIS Chip Card type is switched to available Issuer when field 22 POS Entry Mode code is 05, 07, or 95 and the IAD is greater than 7 bytes.<br>CCD Chip Card type is switched to available Issuer when field 22 POS Entry Mode code is 05, 07, or 95 and IAD bytes 19-32 do not equal binary zero.<br>If Issuer is unavailable, STIP uses Issuer-specified parameters and Issuer-specified response to Acquirer. |

If Issuers respond to an Authorization Request with response code N0 (force to STIP) in field 39 in the 0110 response, VEAS invokes STIP. STIP determines the final response code to send in field 39 in the response message to the Acquirer. The Acquirer receives code 4 in field 44.1 - Response Source/Reason Code; however, the Issuer's advice contains code 6 instead of code 4 in field 44.1 if the Issuer BIN is able to receive enhanced STIP reason codes.

### 7.4.3 Transactions not eligible for STIP

Some transactions can only be approved by the Issuer, and STIP must decline them if the Issuer is unavailable. In these cases, VEAS terminates STIP processing and immediately generates a response. Table 22 lists the conditions under which VEAS terminates STIP processing and generates a response. This **automatic decline** does not apply to Issuer-unavailable Visa Electron Transactions. As noted in the table, Issuers specify in the system files whether STIP is to decline transactions.

**Table 22: Transactions declined in STIP**

| Transactions declined in STIP | | |
|---|---|---|
| **Transaction type** | **Condition** | **STIP response code** |
| ATM Balance Inquiry | Issuer is unavailable and supports ATM balance inquiry transactions. | 91 |
| | Issuer does not support ATM balance inquiry transactions. | 57 |
| POS standalone Balance Inquiry | Issuer is unavailable and supports POS balance inquiry transactions. | 91 |
| | Issuer does not support POS balance inquiry transactions. | 57 |
| Recurring payment | Expired or missing expiry date.[1] | 05 |

| Transactions declined in STIP | | |
|---|---|---|
| **Transaction type** | **Condition** | **STIP response code** |
| Key-entered | Issuer has opted to decline all key-entered transactions (field 22 is not present or the value is 01). | 05 |
| Visa product decline options | Key-entered non-Domestic Transaction.<br>POS transactions, Card-not-present.<br>POS transactions with PIN.<br>**Note** Issuers specify the Decline option in the system files, using the Customer Online Repository (CORE). | 91 |
| | POS transactions without PIN.<br>**Note** Issuers specify the Decline option in the system files (using CORE). | 57 |
| POS with PIN | Issuer has chosen to decline POS transactions with PINs. | 57 |
| Visa Distribution Card | Issuer unavailable. | 91 |
| Large Ticket (Visa Infinite, Visa Signature, or Visa Signature Preferred above USD 99,999.99) | Issuer unavailable. | 91 |
| Mail order/telephone order (MOTO) or Electronic Commerce Transaction (e-commerce) Online Gambling<br>(Field 3 - Processing Code, positions. 1-2 contain 11, field 18 contains 7995, field 25 - Point-of-Service Condition Code contains 01, 08, or 59, and field 60 - Additional POS Information contains 05, 06, 07, 08, 09) | Issuer chooses to decline.[2] | 57 |
| PIN change or unblock (VSDC PIN Management Service; UK-Domestic Transactions only) | Issuer unavailable. | 91 |

1. STIP processes recurring payment transactions the same way it processes MOTO transactions with the recurring payment indicators. Issuers can choose to have STIP approve the recurring payment transactions if the Card expiry date is not present or is present but the date is expired, whether or not the Issuer is available. The default in CORE is NO. For non-participating Issuers, STIP declines recurring payment transactions that have an expired or missing expiry date.

2. Members can choose to have STIP decline all MOTO transactions as well as Online Gambling Transactions. However, Online Gambling Transactions having valid MVVs are sent to the Issuer for processing.

## 7.5 Routing to Issuer

DMSA routes transactions to the Issuer when:

- The Transaction Amount is equal to, or above, the Issuer-specified Issuer limit, or, if applicable, equal to, or above, the mandatory minimum Issuer limit.
- Any of the counts or amounts is equal to or above the Issuer, advice, or activity limits.
- The Issuer performs certain verification services, such as Card Verification Value (CVV) Service, Card Verification Value 2 (CVV2), Cardholder Authentication Verification Value (CAVV) Verification, Dynamic Card Verification Value (dCVV), PIN Verification Service (PVS), or Address Verification Service (AVS).
- The Issuer is in Suppress Inquiry (SI) mode, and the transaction type is one that is allowed to penetrate SI mode.

Members may also select additional routing services, see below for further information.

### 7.5.1 ATM/POS Split Routing Service

The ATM/POS Split Routing Service (and its Alternate Routing option) enables Members to route transactions to different Processing Centres according to the transaction type. For further information, refer to the *Visa Europe Technical Service Descriptions*.

### 7.5.2 ATM Account-Type Split Routing

DMSA and SMS Issuers can specify that the Visa Europe Systems route ATM Transactions based on the account type that the Cardholder selects when using a Card at the ATM. Issuers can specify up to three endpoints: one for deposit accounts; one for credit accounts; and one for universal and non-specified accounts.

For further information, refer to *Visa Europe Routing Services*.

### 7.5.3 PIN/No-PIN Split Routing Service

The PIN/No-PIN Split Routing Service enables Issuers to route all transactions that require PIN Verification to a different Processing Centre from those transactions that do not. For further information, refer to the *Visa Europe Technical Service Descriptions*.

### 7.5.4 Visa Shortest Online Path Service

For Issuers within Visa Europe that process MasterCard purchase or cash transactions using the Visa Shortest Online Path (VSOP) Service, DMSA determines Issuer availability. VEAS routes transactions to available Issuers; if the Issuer is unavailable, then VEAS routes transactions to STIP. For further information and processing requirements, refer to the description of the VSOP Service in the *Visa Europe Technical Service Descriptions*.

### 7.5.5 Gateway Services

Authorization Gateway Services support non-Visa transactions, such as those for MasterCard, Discover, Diners Club, American Express, and Japan Credit Bureau (JCB) International. For further information about Authorization Gateway Services, see the *Visa Europe Technical Service Descriptions* or contact Visa Europe Customer Support.

# 8 Stand-in processing (STIP)

STIP makes authorization decisions to approve or decline transactions on behalf of Issuers.

STIP performs the following tasks:

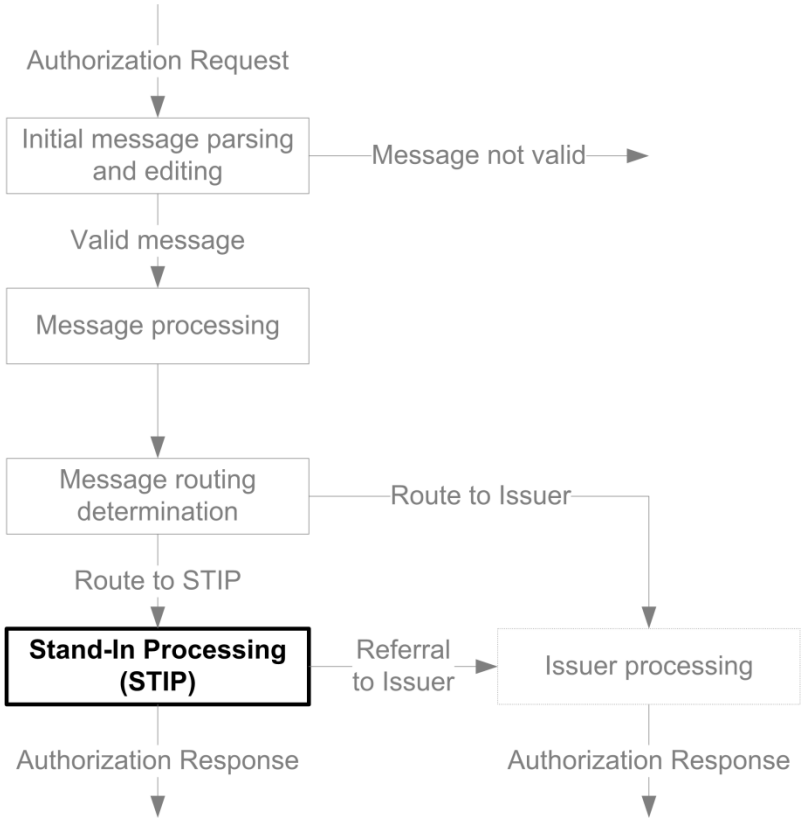
- Evaluates response codes provided by the Issuer
- Performs miscellaneous edits for check digits and expiry dates
- Validates Service Codes
- Performs Exception File checks
- Tests activity
- Determines the highest priority response code
- Performs additional response code conversion, if applicable
- Determines whether to forward the transaction to the Issuer
- Updates activity, if applicable
- Creates an advice for the Issuer, if applicable
- Manages money transfer for Original Credit Transactions (OCTs)

**Note** STIP will convert referral response codes it generates to Decline Response codes based on the transaction type or on regional or Issuer options. VEAS will never respond to an Acquirer with an 01 referral from STIP. If an Issuer from Visa Europe has specified 01 referral for a particular STIP condition, it will always be converted to an 05 decline.

## 8.1 Where STIP fits into the overall DMSA process

Figure 21 illustrates where STIP fits into the overall DMSA process.

**Figure 21: STIP**




## 8.2 STIP initialisation

Before STIP begins its checks, it sets all response codes to 00 to default them to an approval. During STIP processing, STIP invokes several functions depending on Issuer selections, for instance, the PIN Verification Service (PVS), checking expiry dates or the Exception File, and the Card Verification Service for verifying the Cardholder Authentication Verification Value (CAVV), Card Verification Value (CVV), Integrated Card Verification Value (iCVV) or Dynamic Card Verification Value (dCVV).

Each function generates a result code, depending on the Member set-up and on the services the Member uses, and STIP holds these individual interim response codes until it finishes processing the message. STIP then selects the response code with the highest priority and inserts it in field 39 - Response Code.

**Note** In addition to field 39, STIP may include other result code fields, such as field 44.13 - CAVV Results Code, in requests and advices it forwards to Issuers or in responses it sends to Acquirers.

## 8.3 Check Exception File

The following conditions apply to Exception File checking.

- The Exception File can contain:
  - Approval
  - Decline
  - Pick-up
  - Forward-or-approve
  - Forward-or-decline
  - Special response codes A1-A9, or
  - VIP (Very Important Person)

  If an account is in the Exception File with a response code other than the special response codes A1-A9 or VIP, STIP sets the appropriate response code and evaluates it.
- If the Exception File contains response code VIP, VEAS sets the activity limits to the Issuer-specified parameters.
- If the Exception File contains special response codes A1-A9, STIP sets the activity limits as shown in Table 23. If there are no activity limits set in the risk limits file, the limits associated with the A1-A9 special response codes apply. These limits override values specified at the BIN level. DMSA uses the same limits for both subtotal limits and total limits.

Table 23 lists activity limits for the special response codes A1-A9.

**Table 23: Special response code activity limits**

| Special response code activity limits | | | | |
|---|---|---|---|---|
| **Exception File response code** | **1-Day Amount** | **1-Day Count** | **4-Day Amount** | **4-Day Count** |
| A1 | USD 1,500.00 | 3 | USD 1,500.00 | 9 |
| A2 | USD 2,000.00 | 5 | USD 3,500.00 | 12 |
| A3 | USD 3,000.00 | 8 | USD 6,000.00 | 14 |
| A4 | USD 4,500.00 | 12 | USD 8,000.00 | 25 |
| A5 | USD 6,000.00 | 15 | USD 10,000.00 | 40 |
| A6 | USD 8,000.00 | 20 | USD 14,000.00 | 50 |
| A7 | USD 10,000.00 | 25 | USD 20,000.00 | 100 |
| A8 | USD 1,500.00 | 4 | USD 2,000.00 | 10 |
| A9 | USD 2,250.00 | 6 | USD 3,500.00 | 13 |

If the Exception File lists the Account Number of the Cardholder, the value in the action code field determines how STIP processes requests on that account, as specified in Table 24.

**Table 24: Effect of exception records on STIP authorization**

| Effect of exception records on STIP authorization | | |
|---|---|---|
| **Action code** | | **Action taken** |
| 11 | VIP Code | VEAS ignores the results of the Issuer-specified activity count and amount checking. |
| A1-A9 | Other VIP Codes | The action code identifies the special high-value activity limit STIP is to use. |
| 05 | Decline | STIP does not perform activity checking. |
| 04, 07, 41, 43 | Decline and Pick-Up | STIP does not perform activity checking. |
| XA | Forward or Approval | STIP (1) places the action code in the request and (2) sends the request to the Issuer centre. If the centre is not available, STIP checks activity as specified by the centre and assigns a standard approval (code 00) to the request. |
| XD | Forward or Decline | STIP (1) places the action code in the request and (2) sends the request to the Issuer centre. If the centre is not available, STIP assigns a standard decline (code 05) to the request. |

See Appendix A, *Cardholder Database and Advice Files*, for more Exception File information. Refer also to the *DMSA Technical Specifications*.

## 8.4 Evaluate response code

STIP determines the response code based on the following considerations:

- Issuer-specified default response codes
- The default response code override
- CVV or iCVV failure
- CVV2 failure
- CAVV failure
- dCVV failure
- PIN failure
- Visa Smart Debit/Credit (VSDC) Service processing conditions
- $150 rule processing conditions
- Suspected fraud

### 8.4.1 Determine default response code

Issuers can specify default response codes for MCGs at the BIN level. Issuers can specify separate response codes for when the Issuer is available and when it is unavailable. If the Issuer is available, STIP uses the available response code. Otherwise, STIP uses the Issuer-unavailable response code. Issuers can use the following response codes for Issuer-available and Issuer-unavailable conditions:

00 - Approval

01 - Refer to Issuer

04 - Pick up Card

05 - Do not honour

57 - Transaction not permitted to Cardholder

86 - STIP cannot verify PIN

91 - Issuer is unavailable

### 8.4.2 Response codes that override default

The following types of response codes can override default response codes:

- STIP uses the response code specified in the Country-to-Country Embargo table if the Issuer does not specify the default response code.
- The Risky Country table response code. If the Issuer lists the Acquirer country in the Risky Country table, the response code specified by the Issuer in the table overrides the default response code.

The priority in which STIP applies the response codes is:

1. Country-to-Country Embargo table
2. Risky Country table
3. Mandatory minimum limit

**Note** Issuers can establish country-to-country embargo settings for other Card products such as American Express or MasterCard. DMSA controls country-to-country embargoes.

### 8.4.3 Card verification failure - CVV, iCVV, dCVV

If VEAS performs CVV or iCVV verification, and the CVV or iCVV verification fails or cannot be completed, and the Issuer wants STIP to decline transactions under these conditions, STIP assigns response code 05 (decline). Issuers can also choose to have STIP use existing, non-CVV/iCVV-specific parameters for Issuer-unavailable conditions.

**Note** Issuers that use Dynamic Card Verification Values (dCVVs) have similar options. The dCVV verification process is comparable to that for CVV and iCVV verification.

If the transaction is an ATM or POS balance inquiry and the CVV or iCVV failure response code is an approval, STIP changes the response to a decline (05).

See Appendix B.4.1, *CVV and iCVV* and Appendix B.5, *Contactless processing (dCVV)*, for more information.

### 8.4.4 Card verification failure (Card-not-present) - CVV2

A CVV2 is a 3-digit number on the back of a Card used in a cryptographic procedure to verify Card authenticity. If STIP detects a CVV2 failure during stand-in processing, STIP responds to the Acquirer with the CVV2 failure response code (00, 05 or N7) pre-selected by the Issuer. STIP also returns code N in field 44.10 - CVV2 Results Code for Acquirers certified to receive the field. (Visa Europe recommends this certification.)

See Appendix B.4.2, *CVV2*, for more information.

### 8.4.5 Verified by Visa failure - CAVV

If VEAS performs CAVV validation, and the CAVV validation fails or VEAS cannot complete the process, and the Issuer wants STIP to decline transactions under these conditions, STIP assigns response code 05 (decline). Issuers can also choose to have STIP use existing, non-CAVV-specific parameters for Issuer-unavailable conditions.

STIP responds to CAVV transactions as follows:

- If the Issuer participates in the Verified by Visa Service, and STIP does not complete the CAVV validation process, and the Issuer has chosen to decline such transactions, STIP generates response code 05 as a high-priority value
- If the CAVV is invalid and the Issuer has chosen to decline such transactions, STIP generates response code 05 as a high-priority value

VEAS accepts Authorization Requests and full financial requests submitted with both a CAVV and a CVV2. When VEAS receives a request containing both a CAVV and a CVV2, the CAVV validation result takes precedence over the other risk control's verification result. This priority processing also applies to Issuer-unavailable transactions sent to STIP: if the CAVV passes but the CVV2 fails, STIP does not decline the transaction because of the CVV2 failure.

When a CAVV and a CVV2 are present, VEAS validates the CAVV first:

- If the CAVV validation is successful, VEAS verifies the CVV2, and forwards both results to the Issuer and to the Acquirer in the response. (The CVV2 result is contained in field 44.10; the CAVV result is contained in field 44.13.)
- If the CAVV validation fails, CAVV verification rules apply:
  - If the Issuer specifies that VEAS is to decline all transactions that fail the CAVV check, VEAS declines the transaction without verifying the CVV2
  - If the Issuer specifies that VEAS is to forward all results to the Issuer regardless of the outcome, VEAS validates the CVV2 and includes both field results in the request to the Issuer

  **Note** If the Issuer approves the Authorization Request that contains a successful CAVV result, the Issuer may not submit a Chargeback for reason code 23 (T&E - invalid transaction) or 61 (fraudulent mail/telephone order transaction).

If STIP validates the CAVV in a request that includes a CVV2 value:

- If the CAVV value is valid, STIP validates the CVV2 value and follows the Issuer's CVV2 STIP parameter rules
  - If the CAVV value is valid but the CVV2 value fails verification, the CAVV result takes precedence and STIP follows the CAVV-related processing specifications
- If the CAVV validation fails, STIP declines the transaction without validating the CVV2

If STIP cannot complete the CAVV validation process, STIP still uses the Issuer-specified CAVV processing parameters:

- If STIP is to continue processing, it verifies the CVV2 according to the related processing parameters
- If STIP is to decline the transaction if CAVV validation fails, STIP validates the CVV2 and sends a Decline Response

**Note** For further information about VEAS processing when both elements are present in a request, refer to the description of the Verified by Visa Service in the *Visa Europe Technical Service Descriptions*.

See Appendix B.17, *Verified by Visa Service and Electronic Commerce Transactions (CAVV)*, for more information.

### 8.4.6 PIN verification failure

If the transaction fails PIN Verification by the PVS, VEAS saves response code 55 (incorrect PIN) in the PVS response code field. If the number of allowable invalid PIN-entry attempts is exceeded, VEAS saves the interim response code 75 (allowable number of PIN-entry tries exceeded) instead and converts it to response code 05, although it forwards response code 75 to the Issuer in the 0120 advice. If the Issuer returns response code 75 in field 39 of the 0110 response, VEAS forwards the field 39 response code unchanged to the Acquirer; otherwise, VEAS inserts response code 05 in field 39 before forwarding the response to the Acquirer.

VEAS records each incorrect PIN-entry attempt and accumulates the total in the Activity File in the Cardholder Database. For an explanation of VEAS processing when the number of unsuccessful PIN-entry attempts exceeds the Issuer-set limit, refer to the description of the PIN Verification Service (PVS) in the *Visa Europe Technical Service Descriptions*.

If the transaction is POS (not ATM or cash) and the Issuer has not chosen to have VEAS perform PIN Verification, STIP sets the PIN Verification response code to 86, or immediately replies to the transaction with response code 57 (transaction not permitted to Cardholder) if the Issuer has selected this option.

### 8.4.7 VSDC response code

During Chip Transaction processing, Issuers can select a response code, depending on the error condition encountered. Currently, Issuers can specify response codes for 28 different conditions. For example, if the transaction has exceeded the Floor Limit that condition is flagged by the VSDC data in the request, and the Issuer can select an Approval Response or Decline Response for stand-in processing.

Some Issuers have a Referral Response set for some VSDC STIP options. The Referral Response is no longer allowed, and Visa changes referrals to the default response if the Issuer does not request a change to their Visa System parameters.

See Chapter 2, *Overview of DMSA and the Visa Europe System*, for basic information about VSDC processing. Also refer to the description of the Visa Smart Debit/Credit (VSDC) Service in the *Visa Europe Technical Service Descriptions*, and to *the Visa Smart Debit/Credit System Technical Manual*.

### 8.4.8 $150 Rule response codes

The $150 rule applies to purchase transactions that are for USD 150.00 or less. When an Issuer is unavailable for low-risk transactions and activity limits have been exceeded, STIP can override a Decline Response to an Acquirer with an Approval Response. Issuers can specify different response codes for different risk levels if Issuers are using risk levels to classify Cardholders. Table 25 shows the MCGs eligible for the $150 rule.

**Table 25: MCGs eligible for the $150 rule**

| MCGs eligible for the $150 rule | | | |
|---|---|---|---|
| **MCG** | **Description** | **Eligible** | **Not eligible** |
| 01 | Airline | X | |
| 02 | Lodging | X | |
| 03 | Auto Rental | X | |
| 04 | Restaurant | X | |
| 05 | Other Purchase | X | |
| 06 | MOTO/e-commerce | | X |
| 07 | Risky Purchase | | X |
| 08 | Other Cash | | X |
| 09 | ATM Cash | | X |

The $150 rule does not apply to:

- Automated dispensing machine (ADM) transactions
- Risky purchase transactions
- Visa Electron Transactions: VEAS generates response code 05 in field 39 if the activity amount or the activity count is exceeded

The $150 rule applies to both Domestic Transactions and International Transactions. It is mandatory for US Issuers.

### 8.4.9 Suspected fraud

When Issuers respond to an 0100 Authorization Request, they can use response code 59 in field 39 to alert Visa to suspected fraud. VEAS changes code 59 to code 05 (decline) before forwarding the 0110 response to the Acquirer. The usage of code 05 minimises the possibility of problems between the Merchant and the Cardholder.

## 8.5 Miscellaneous edits

When applicable, STIP verifies Account Numbers, expiry dates, and Account Number lengths. If they are invalid, STIP responds as follows:

- Invalid Account Number check digit: If the Issuer has chosen to have VEAS edit for the Luhn modulus-10 check digit and the check digit fails validation, STIP generates response code 14 (invalid Account Number [no such number]).
- Expiry date edits:
  - If the expiry date is present, STIP validates that the date is a valid YYMM value and that it is not earlier than the current date. If the expiry date is invalid, STIP generates response code 54 (expired Card) for the response.
  - If the transaction is MOTO/e-commerce and the Issuer does not allow MOTO/e-commerce transactions without an expiry date in Issuer-unavailable situations, STIP generates response code 05 for the response.

**Note** See Section 8.5.2, *Expiry date check*, for further information.

- Account Number length check: If the Account Number length is wrong (that is, the Account Number length does not match the valid range of account lengths allowed for the Issuer BIN), STIP uses response code 14 (invalid account number) for the response.

VEAS bypasses the expiry date check for reversals and for Visa Electron Transactions.

### 8.5.1 Mod-10 check

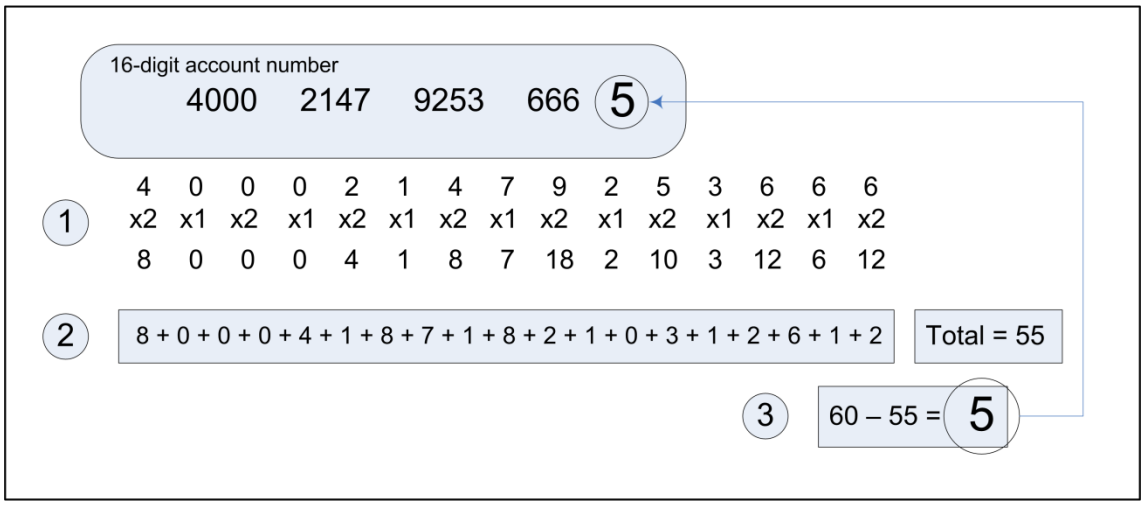
STIP does not perform Account Number verifications on alphanumeric Account Numbers (non-standard Account Numbers) or for Account Numbers in Exception File update messages.

VEAS uses the Luhn modulus-10 algorithm to determine or to verify the last digit of the Account Number as follows:

1. Working right to left, starting with the next-to-last digit, VEAS multiplies every other number by 2. Starting with the second-to-last number, VEAS multiplies every other number by 1.
2. VEAS calculates the sum of the digits of the values created in step 1.
3. From the next higher multiple of 10, VEAS subtracts the sum from step 2. The result is the check digit (the last digit of the Account Number). If the result is a multiple of 10 (ends in a zero), the check digit is zero.

Figure 22 illustrates the calculation process that VEAS uses to calculate the check digit for a 16-digit Account Number.

**Figure 22: Modulus-10 check digit algorithm calculation example**




### 8.5.2 Expiry date check

STIP edits expiry dates depending on whether the expiry date is present in the message in field 14 - Date, Expiration, and whether the Issuer has established that STIP can process MOTO/e-commerce transactions (field 25 - Point-of-Service Condition Code contains 08) without expiry dates. Expiry dates must be in a valid YYMM numeric format: YY = year (00-99), and MM = month (01-12).

VEAS considers a field 14 expiry date to be expired if it is 50 years greater than the current date.

If the expiry date is invalid or has expired, STIP sets the expiry date response code to 54, and sets the internal indicator to indicate that the transaction should be forward-referred to the Issuer, if available. VEAS includes the response code in 0110 responses from STIP as well as in STIP advices.

If the expiry date is not present and the transaction meets one of the following qualifications, STIP sets the expiry date response code to 05, and sets an internal indicator to indicate that the transaction should be forward-referred to the Issuer, if available:

- It is not a MOTO/ e-commerce transaction (field 25 does not contain 08 or 59)
- It is not a Visa Electron Transaction
- It is a MOTO/e-commerce transaction (field 25 contains 08 or 59) and the Issuer has established that it does not want VEAS to approve MOTO/e-commerce transactions in STIP that do not have an expiry date

  If Issuers instruct VEAS to process MOTO/e-commerce transactions that lack an expiry date, VEAS always tries to forward the transaction to the Issuer. If the Issuer is unavailable, STIP uses Issuer-established parameters to process the transaction. This procedure does not apply to transactions involving expired Cards.

#### 8.5.2.1 Manually prepared authorizations without expiry dates

STIP processes Manual Authorization Requests (field 22 contains 01) that lack expiry dates as follows:

1. VEAS declines the request with response code 05 (do not honour) in field 39 if:
   - The Issuer Processor is unavailable or times out, and/or
   - The transaction is anything but MOTO/e-commerce, or the transaction is MOTO/e-commerce, and the Issuer BIN option requires that MOTO/e-commerce transactions include the expiry date
2. VEAS inserts response code 05 in field 39 and forwards the request to the Issuer Processor for approval if all of the following conditions exist:
   - The request is below the Issuer limit, and
   - The transaction is anything but MOTO/e-commerce, or the transaction is MOTO/e-commerce, and the Issuer BIN option requires that MOTO/e-commerce transactions include the expiry date
3. If the Processing Centre of the Issuer approves the request, it changes the response code in the response message before it returns it to DMSA.

## 8.6 Perform activity checks

STIP determines activity limits and performs activity checking.

**Note** DMSA does not check activity and does not update the Activity File if the Transaction Amount is below the Issuer-specified advice limit amount. (SMS performs activity checking only if the Issuer has specified a value other than zero for the Issuer BIN's activity count.)

### 8.6.1 Exception rules

STIP does not act on activity checking results if the highest priority response code already indicates a decline when the transaction enters STIP. STIP also does not check activity for transactions that meet the following qualifications:

- Account Verification and address verification transactions
- Below-advice-limit transactions for 0100 requests
- Repeat transactions (message type 0101)
- If the transaction is between limits and if mandatory minimum limits apply with a non-zero Issuer limit, STIP tests activity; however, if the Issuer BIN indicates no activity checking for between-Issuer limits and advice limits, STIP does not test activity

### 8.6.2 Activity limit determination

STIP uses the following parameters to determine a transaction's applicable activity limit:

- Issuer-specified activity limits for the applicable Merchant Category Group (MCG) and Total Purchase or Total Cash levels
- Mandatory minimum activity limits for the applicable MCG and Total Purchase or Total Cash levels
- Any optional Issuer-exempt overrides for the mandatory minimum limits
- Transaction jurisdiction (domestic or international) and Issuer region
- Issuer-available or Issuer-unavailable condition

Issuers must specify activity limits (count, amount, and a 4-day multiplier, which can be any value between 1 and 4 in increments of .05), at least for Total Purchase and for Total Cash. However, unlike Issuer limits, Issuers do not have to specify activity limits for each of the 11 MCGs. If Issuers choose to specify activity limits (count, amount, and 4-day multiplier) for the MCGs, they can pick and choose among the 11 MCGs.

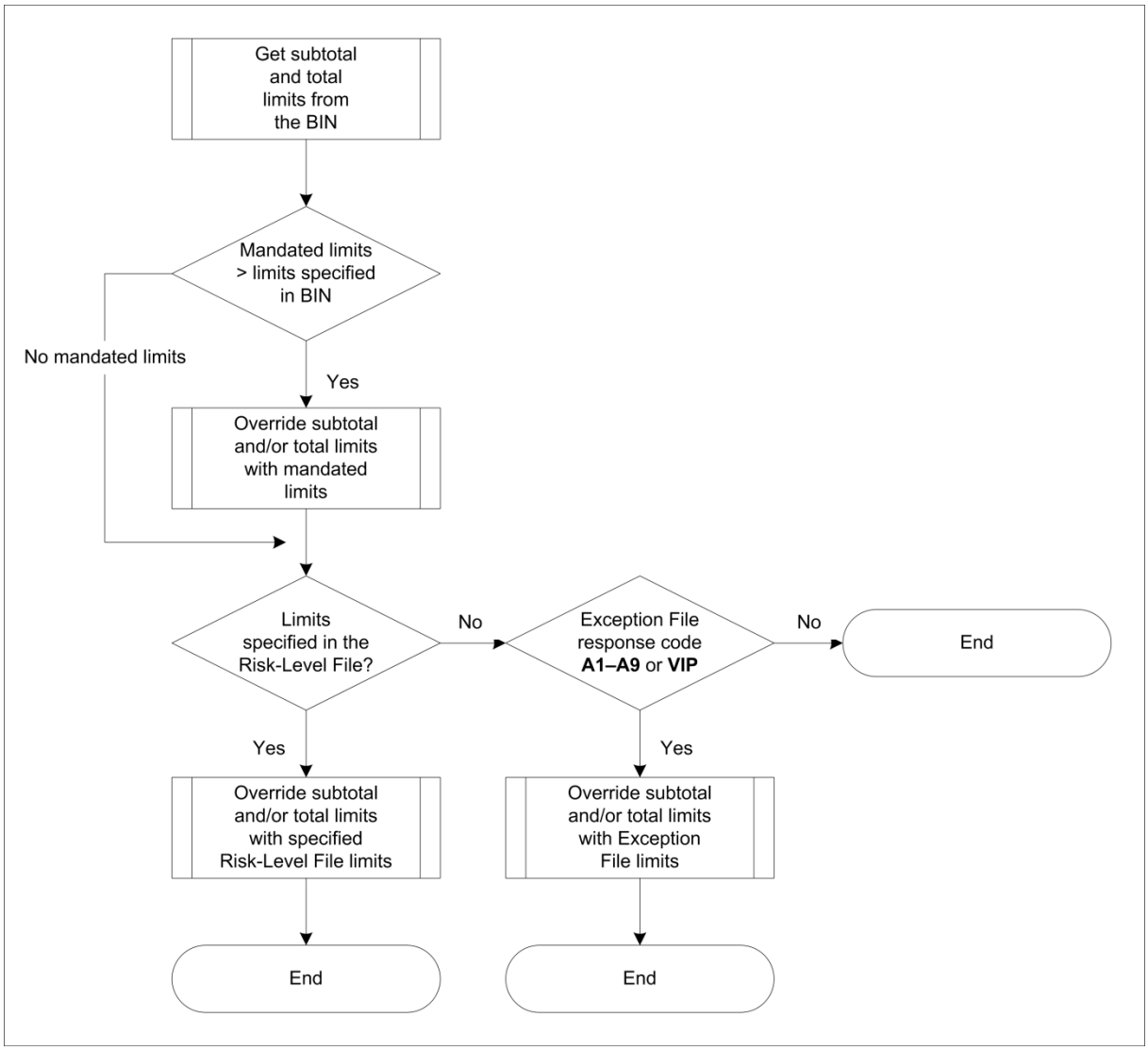
If an Issuer does not establish an activity limit for an MCG, STIP uses the activity limit's count, amount, and 4-day multiplier for the corresponding totals.

Separate activity limit sets exist for Issuer-available and Issuer-unavailable conditions. VEAS uses Issuer-unavailable activity limits when the Issuer has signed off, when the Visa Europe System thinks the Issuer is offline, or when a transaction sent to the Issuer times out.

Figure 23 illustrates how VEAS determines activity limits.

**Note** Figure 23 illustrates a general flow that shows how STIP determines activity limits. This flow does not show exception scenarios.

**Figure 23: Activity limits determination**




## 8.6.3 Limit selection hierarchy

When Issuers establish limits at multiple levels, STIP uses the hierarchy in Table 26 to determine processing parameters.

**Table 26: Activity limit selection hierarchy**

| Activity limit selection hierarchy | | |
|---|---|---|
| **These limits** | **Supersede the following** | **Under these circumstances** |
| Default risk-level BIN limits | n/a | Never - The default BIN-level, risk-level limit never overrides any other limit. |
| Non-default risk-level limits | Default risk-level BIN limits | Always |
| MM activity limits | Non-default risk-level limits other than those for risk level D | When MM limits apply and the Visa MM activity limit is higher than the Issuer-specified activity limit. |
| | Default risk-level BIN limits | |

| Activity limit selection hierarchy | | |
|---|---|---|
| **These limits** | **Supersede the following** | **Under these circumstances** |
| Account-specific limits | MM activity limits | Always |
| | Non-default risk limits | |
| | Default risk-level BIN limits | |

### 8.6.4 Testing activity

STIP tests activity as follows:

- If the Issuer specifies the subtotal limit, STIP checks the subtotal limit. STIP uses previous subtotal values (1-day count and amount and 4-day count and amount) from the Activity File.
- If the Issuer specifies the total limit, STIP checks the total limit. STIP calculates the previous total values (1-day count and amount and 4-day count and amount) by adding subtotal values from the Activity File.
- STIP adds the current Transaction Amount to the previous total values and compares them with the limits in the following order:
  1. 1-day total amount
  2. 4-day total amount
  3. 1-day total count
  4. 4-day total count

To determine the maximum activity (count and amount) allowed over four days, STIP multiplies the 1-day count and amount limits by the 4-day multiplier to determine the 4-day count and amount limits. The multiplier can be any value between 1 and 4, in increments of .05. STIP raises fractional results on the calculation of the count limit to the next higher integer. For instance, a 1-day count of 2 multiplied by a 4-day multiplier of 2.1 would yield a 4-day count of 4.2, which STIP would round up to 5.

If any activity exceeds Issuer-specified activity limits, STIP forwards the transaction with an over-limit code to the Issuer for an authorization decision. If the activity is within the Issuer-specified activity limit, STIP continues processing the transaction.

If only the subtotal limit applies, STIP does not perform the total limit checks.

- The subtotal limit only applies to the following MCGs:

  1 - Airline

  2 - Lodging

  3 - Auto Rental

  4 - Restaurant
- If the Transaction Amount or count is exceeded, STIP responds as follows:
  - Transaction Amount is exceeded - STIP generates response code 61
  - Transaction count is exceeded - STIP generates response code 65

STIP performs activity checking in conjunction with other tests. T&E MCG transactions fail activity checking when they fail both the MCG test and the Total Purchase test. STIP does not

approve transactions passing activity checking but failing the other tests and does not perform activity accumulation.

### 8.6.5 Testing activity for T&E Transactions

A T&E Transaction must pass activity checking for the appropriate MCG or for Total Purchase. (A T&E Transaction fails only if it fails both the MCG and Total Purchase activity checks.) VEAS checks MCG activity limits before it checks Total Purchase activity limits:

- If activity limits exist for the MCG in question, and if the Transaction Amount is below them, VEAS increments the MCG's count and amount accumulators and approves the transaction.
- If activity limits exist for the MCG in question but the transaction exceeds them, VEAS checks the Total Purchase activity limits. If the Transaction Amount is below these limits.

VEAS approves the transaction and increments the MCG accumulators:

- If Visa mandatory minimum (MM) limits apply to a transaction, STIP uses the greater of Issuer-specified or MM activity limits and if the transaction passes, updates the accumulators of the limits it uses
- If MM activity limits do not apply to the transaction and if the Issuer does not specify activity limits for the MCG in question, STIP only performs Total Purchase activity checking and updates the count and amount accumulators for the MCG in question if the transaction is approved

  **Example:**

  An Issuer specifies 1-day activity limits of USD 500.00 for Commercial Travel and USD 300.00 for Total Purchase.

  A transaction of USD 350.00 for Airline will pass the activity check because, although it exceeds the Total Purchase limit, it is within the Commercial Travel 1-day limit. At this point, the accumulated activity both for Commercial Travel and for Total Purchase is USD 350.00.

  However, a second transaction of USD 200.00 for Airline will not pass the activity check because, with the USD 350.00 activity previously approved, it exceeds both the Total Purchase and Commercial Travel limits.

### 8.6.6 Testing activity for non-T&E Transactions

Non-T&E activity checking and accumulation applies to transactions that do not belong in the Commercial Carrier, Lodging, Auto Rental, or Restaurant MCGs.

If activity limits exist for the MCG in question, and if the Transaction Amount is below them, DMSA increments the MCG's count and amount accumulators and approves the transaction. If there are MCG activity testing limits for non-T&E Transactions, the transaction must pass to be approved.

If activity limits exist for the MCG in question, and if the Transaction Amount is below them, DMSA increments the MCG's count and amount accumulators and approves the transaction. If there are MCG activity limits, the transaction must pass them for DMSA to approve it.

If activity limits do not exist for the MCG in question, STIP checks the Total Purchase activity limits. If the Transaction Amount is below the limits, DMSA increments the Total Purchase

count and amount accumulators and approves the transaction; otherwise, DMSA does not approve the transaction.

If activity limits exist for the MCG in question and for Total Purchase, non-T&E Transactions must pass both activity checks.

MOTO/e-commerce and Risky Purchase - STIP checks both the MCG-level activity limits, if the Issuer establishes them, and the Total Purchase activity limits. If the Issuer establishes both limits, the transaction must pass both checks. If the Issuer establishes only the Total Purchase activity limits, the transaction must pass that check. DMSA updates the MCG-level activity limit and Total Purchase activity limit accumulators as appropriate.

Medical and Other Purchase - DMSA checks the Issuer-specified Total Purchase activity limits and updates the Total Purchase activity accumulators if the transaction passes. Issuers cannot specify MCG-level activity limits for these MCGs. For transactions that fall within the Other Purchase MCG, STIP compares the mandatory minimum activity limit with the Issuer-specified Total Purchase activity limit and selects the higher of the two for checking the transaction's activity. When DMSA completes activity checking, it updates the activity accumulators accordingly.

**Example:**

An Issuer specifies 1-day activity limits of USD 100.00 for Mail Order/Telephone Order transactions and USD 300.00 for Total Purchase.

A transaction of USD 50.00 for a mail order purchase will pass the activity check because it is within both the Mail Order/Telephone Order and Total Purchase 1-day limits. At this point, the accumulated activity for both Mail Order/Telephone Order and Total Purchase is USD 50.00.

However, a second transaction of USD 100.00 for a mail order purchase will not pass the activity check because, with the USD 50.00 activity previously approved, it exceeds the Mail Order/Telephone Order limit, even though it is within the Total Purchase limit.

### 8.6.7 Testing activity for cash transactions

Activity-checking rules for cash transactions depend on whether the transaction is an ATM MCG or if it is a Quasi-Cash or Other Cash MCG. Issuers must establish activity limits for Total Cash. Issuers can, if they choose, establish activity limits for the ATM Cash MCG. Issuers do not establish activity limits for Quasi-Cash or Other Cash MCGs.

ATM Cash - If activity limits exist for the ATM Cash MCG, the transaction must pass both the ATM Cash MCG limits and the Total Cash activity limits. If the transaction passes, DMSA increments the ATM Cash MCG and Total Cash count and amount accumulators and approves the transaction.

If the Issuer does not specify activity limits for the ATM Cash MCG, DMSA checks the Transaction Amount against the Total Cash activity limits. If the transaction passes the Total Cash check, DMSA increments the Total Cash count and amount accumulators and approves the transaction.

Uniquely for ATM Cash, it is possible to set ATM sub-limits that are greater than the Total Cash limit; the Total Cash limit could even be zero. In such an instance, STIP uses the ATM sub-limits solely instead of the Total Cash limit.

Quasi-Cash and Other Cash MCG - DMSA uses the Total Cash activity limits. DMSA checks Quasi-Cash and Other Cash MCG transactions against the activity limits the Issuer establishes for Total Cash and updates activity accumulators for Quasi-Cash and Other Cash MCG transactions. Issuers cannot specify MCG-level activity limits for Quasi-Cash and Other Cash MCGs.

**Example:**

An Issuer specifies 1-day activity limits of USD 100.00 for ATM and USD 300.00 for Total Cash.

A transaction of USD 50.00 for ATM will pass the activity check because it is within both the ATM and Total Cash 1-day limits. At this point, the accumulated activity for both ATM and Total Cash is USD 50.00.

However, a second transaction of USD 100.00 for ATM will not pass the activity check because, with the USD 50.00 activity previously approved, it exceeds the ATM limit, even though it is within the Total Cash limit.

## 8.7 Check service code

A Service Code is a 3-digit number encoded on Track 1 and on Track 2 of the magnetic stripe that identifies the circumstances under which the Card can be used. Service Code edit conditions are as follows:

- VEAS performs Service Code edits only for Visa Cards and Visa Electron Cards
- If the Service Code is invalid, STIP generates response code 57
- If the Service Code indicates that it is not valid for an International Transaction and the transaction is international, STIP generates response code 57
- If the Service Code indicates that it is not valid for ATM Transactions and the transaction is ATM, STIP generates response code 57

For a list of valid Service Codes, refer to the latest edition of the *Payment Technology Standards Manual*.

## 8.8 Finalise response code

STIP compares all response codes generated so far and selects the one with the highest priority (indicating the most risk or the greatest message error). If the current response code has a higher priority, STIP keeps it. Otherwise, STIP replaces it with one from the following list:

- Issuer default response code
- Risky Country table response code
- PIN Verification Service (PVS) response code
- Expiry date edit response code
- CVV or iCVV response code
- CAVV response code
- dCVV response code
- Exception File response code

## 8.9 Forward-referral to the Issuer

STIP can forward-refer a transaction to the Issuer, which means that STIP sends the transaction to the Issuer with the STIP-selected response code in field 39 - Response Code. The Issuer then has the option to approve or decline the transaction.

If the transaction does not qualify for forward-referral to the Issuer, STIP can respond to the Acquirer on the Issuer's behalf.

### 8.9.1 Forward-refer qualifications

A transaction must meet the following conditions for STIP to forward-refer it to the Issuer.

- Prerequisites:
  - The Issuer must be available
  - The Issuer must choose at the Processor level to accept forward referrals
  - The response code must indicate that the transaction is eligible for forward-referral
- For CVV Service processing, if the Issuer chooses the **All Respond** option, VEAS validates the CVV or iCVV; if the validation fails, VEAS responds to the Acquirer with the Issuer's invalid CVV/iCVV response code.
- For CVV2 Service processing, if the Issuer chooses the **CVV2 All** option, VEAS validates the CVV2; if the validation fails, VEAS forwards the request to the Issuer with the CVV2 in field 126.10 - CVV2 Authorization Request Data. If the Issuer is unavailable, VEAS responds to the Acquirer with the Issuer's CVV2 response code.
- The transaction is an ATM cancellation (or reversal) transaction.
- The transaction is a MOTO/e-commerce transaction in which the expiry date is not present and the Issuer chooses not to process MOTO/e-commerce transactions in STIP without an expiry date.
- The Account Number length is invalid (not one of the Card lengths specified for the Issuer BIN).

### 8.9.2 No Forward-refer processing

If a transaction does not qualify for forward-referral, VEAS processes it as follows:

- If the transaction exceeds the activity amount or count, the Transaction Amount is below USD 150.00, and the Issuer has chosen a POS referral conversion response code for transactions below USD 150.00, STIP uses the highest priority response code
- If the transaction exceeds the activity amount or count, but the $150 rule does not apply, then STIP will respond to the Acquirer with a 05 (decline) as described in Section 8.6, *Perform activity check*
- If the transaction exceeds the activity amount or count, and the account is a Visa Electron account, STIP forces the response code to 05

## 8.10 Update Activity accumulators

STIP updates the count and amount activity information in the Activity File under the following conditions:

- The transaction is approved in STIP

- The transaction is an authorization and not a repeat (message type 0101)
- The transaction is not a verification transaction
- The transaction is not below the advice limit
- The transaction is between advice and Issuer limits and the Issuer chose to have STIP check activity

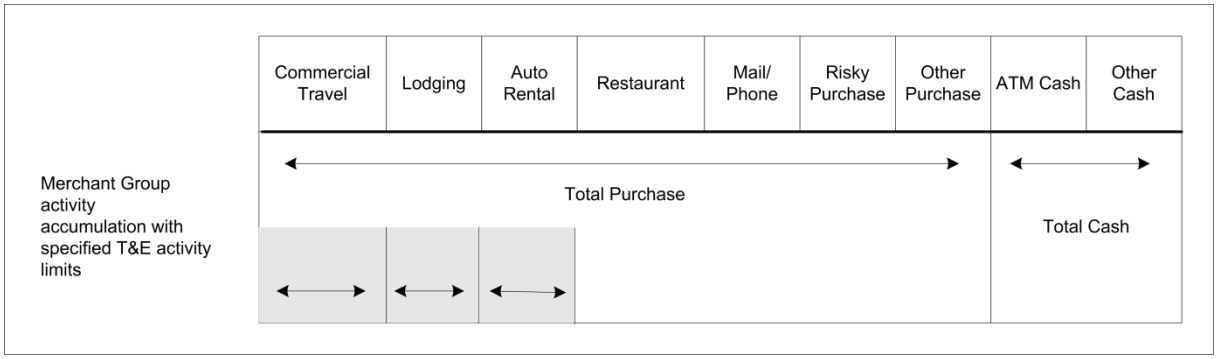
See Section 8.13.1, *Reversal processing*, for information about processing reversals.

VEAS accumulates activity in one of two categories: Total Purchase or Total Cash. If the Issuer selects activity limits for any Merchant group within either of these two categories, VEAS accumulates activity once for the MCG only.

For example, Figure 24 illustrates how VEAS accumulates activity for an Issuer that has selected separate activity limits for Commercial Travel, Lodging, and Auto Rental MCG transactions.

VEAS accumulates activity in any of these groups for that group and for Total Purchase.

**Figure 24: Example of activity accumulation**




## 8.11 Create advice

Issuer options and the results of STIP processing determine whether STIP sends an advice to the Issuer. The following conditions affect advice creation:

- STIP does not create advices:
  - For below-advice-limit transactions that are approved
  - For MasterCard or American Express transactions
  - For transactions receiving any of the response codes listed in Table 27

**Table 27: No-advice STIP Decline Response codes**

| No-advice STIP Decline Response codes | |
|---|---|
| **Response code** | **Explanation** |
| 06 | Error |
| 12 | Invalid transaction |
| 13 | Invalid amount |
| 14 | Invalid account |
| 15 | No such Issuer |

| No-advice STIP Decline Response codes | |
|---|---|
| **Response code** | **Explanation** |
| 28 | File temporarily unavailable |
| 57 | Transaction not permitted to Cardholder |
| 62 | Restricted Card; restricted between certain countries |
| 63 | Security violation |
| 78 | No account |
| 81 | PIN cryptographic error found |
| 96 | System malfunction |
| N3 | Cash back service not available |
| N4 | Cash request exceeds Issuer limit |

- STIP creates advices for between-advice-limit and Issuer-limit transactions when the Issuer specifies that STIP is to create advices for those conditions.

**Note** STIP creates advices for all non-approved PCAS transactions.

Table 28 shows how STIP determines whether to create advices for non-approved PCAS between-limit transactions.

**Table 28: Advice creation for non-approved PCAS between-limit transactions**

| Advice creation for non-approved PCAS between-limit transactions | |
|---|---|
| **CORE setting** | **STIP decision** |
| Activity Testing On | Selecting YES or NO determines whether STIP is to check activity limits for between-limit transactions. When activity exceeds Issuer-specified activity limits, STIP forwards the Authorization Request to the Issuer for a response. |
| Advice Creation On | For PCAS participants, selecting YES or NO determines whether STIP is to create advices for approved between-limit transactions. STIP creates advices for all non-approved PCAS transactions. |

## 8.12 Convert response code for Merchant

STIP converts response codes under the following conditions:

- When there is a CVV error (response code 82) and PIN-entry activity is exceeded (response code 75), STIP forwards the transaction with these response codes to the Issuer. The response code to the Acquirer contains an approval or Decline Response code specified by the Issuer in the system tables. If STIP assigns interim response code 75 to the transaction, VEAS converts it to 05 but sends response code 75 to the Issuer in the 0120 advice. If the Issuer returns response code 75 in the 0110 response, VEAS forwards it unchanged to the Acquirer; otherwise, VEAS inserts response code 05 in field 39 before sending the message to the Acquirer.

- If the response code is a referral (01 or 02) and the transaction is from an unattended terminal (field 25 - Point-of-Service Condition Code contains 02), STIP converts the response code to 05.
- If the response code is a referral (01 or 02) and the transaction is equal to or less than USD 500.00, and the transaction is regional or interregional, STIP converts it to 05.

**Important** In the Visa Europe System, STIP converts all referral response codes to declines regardless of the amount.

When STIP creates an advice for the Issuer, STIP inserts the original, unconverted response code in field 39 of the advice.

### 8.12.1 Converting over-limit and referral codes in Acquirer responses

STIP converts over-limit response codes 61 and 65 to Approval Response or Decline Response codes as the Processing Centre of the Issuer specifies. Table 29 contains conversion details.

**Table 29: Converting over-limit and referral codes response**

| Converting over-limit and referral codes response | | |
|---|---|---|
| **Code** | **Condition** | **Converted to...** |
| 01 | Exception File purchase referrals from POS terminals | Issuer-specified approval code 00 or decline code 05. Non-US Issuers may specify referral code 01 except for Visa Electron Transactions, which cannot be referred per Visa Europe Operating Regulations. |
| | ATM Transaction referrals | Decline code 05. |
| 61 ,65 | Over-limit purchases from electronic terminals | Referral. For POS transactions with amounts under USD 150.00 (the $150 rule), Issuers may specify approval code 00 or decline code 05. STIP uses these Issuer-specified response codes if field 60.1 - Terminal Type and field 60.2 - Terminal Entry Capability are not zero-filled. For more information see the description of field 39 - Response Code in the DMSA Technical Specifications. |
| 75 | Exceeds PIN-entry retry limit (any transaction) | Decline code 05.[1] |

1. Although VEAS converts response code 75 to decline code 05, VEAS forwards response code 75 to Issuers in 0120 advices. If an Issuer returns the 0110 response with response code 75 in field 39, the Visa Europe System forwards it unchanged to the Acquirer. Otherwise, VEAS inserts decline code 05 in field 39 before sending the response to the Acquirer.

STIP also converts other response codes before it sends the response message to Acquirers.

Table 30 contains these conversion details.

**Table 30: Converting approval, forward-or-approve/decline, or incorrect CVV or iCVV response codes**

| Converting approval, forward-or-approve/decline, or incorrect CVV or iCVV response codes | | |
|---|---|---|
| **Response code** | **Condition** | **Converted to** |
| 11<br>A-A9 | VIP (Very Important Person) approval (Authorization Request) | Approval code 00. |
| | VIP approval (Account Number verification - Visa US only) | Not declined, code 85. |
| XA | Forward or approve (Authorization Request) | Approval code 00. |
| | Forward or approve (Account Number verification - Visa US only) | Not declined, code 85. |
| XD | Forward or decline | Decline code 05. |
| 82 | Incorrect CVV, iCVV, or dCVV | One of the following Issuer-specified codes:<br>00 = Approval code<br>01 = Referral code<br>04 = Pick Up code<br>05 = Decline code |

Acquirers receive declines (code 05, do not honour) instead of Referral Responses (code 01, refer to Card Issuer, or code 02, refer to Card Issuer, special condition) in certain interregional and regional STIP, MOTO, Automated Fuel Dispenser (AFD), computer network services, door-to-door sales, unattended terminal, and impractical Merchant environment transactions that are conducted using a Visa Card. Table 31 defines the processing rules for Referral Response codes.

**Note** In the Territory, these referral-to-decline conversion rules apply to Domestic Transactions as well as to regional and interregional transactions.

**Table 31: Referral Response code processing rules**

| Referral Response code processing rules | |
|---|---|
| **Condition** | **Rule** |
| STIP processes the transaction and all of the following is true:<br>■ The STIP-generated Referral Response code is 01 or 02[1].<br>■ The Issuer is available and the STIP parameter indicates that the Issuer accepts forward referrals.<br>■ For all regions except Visa Europe, the Transaction Amount is equal to or less than USD 500.00. If the Issuer is in the Visa Europe region, a threshold amount does not apply. | The Visa Europe System forwards the transaction to the Issuer for authorization. |
| STIP processes the transaction and all of the following is true:<br>■ The STIP-generated Referral Response code is 01 or 02<br>■ The Issuer is available and the STIP parameter indicates that the Issuer does not want forward referrals<br>Or<br>■ The Issuer is unavailable.<br>■ For all regions except Visa Europe, the Transaction Amount is equal to or less than USD 500.00. If the Issuer is in the Visa Europe region, a threshold amount does not apply. | VEAS changes the Referral Response code 01 or 02 to Decline Response code 05 in the response to the Acquirer. |
| The Issuer returns Referral Response code 01 or 02 and one of the following is true:<br>■ The POS condition code is 08<br>■ The POS condition code is 02 (unattended terminal)<br>■ The MCC in field 18 - Merchant Type indicates a MOTO, AFD, computer network services, or door-to-door sales transaction<br>■ The MCC in field 18 indicates a transaction from an impractical Merchant environment as defined in the *Visa Europe Operating Regulations*, and the Transaction Amount is equal to or less than USD 100.00 | VEAS changes Referral Response code 01 or 02 to Decline Response code 05 in the response to the Acquirer. |

1. STIP or the Issuer can generate forward-referral codes 01 and 02. STIP or the Issuer can send forward-referral code 01 to the Acquirer in the response. Only the Issuer can send forward-referral code 02 to the Acquirer in the response.

## 8.13 Special considerations

### 8.13.1 Reversal processing

DMSA does not match a reversal to the original. DMSA also does not know how the original was processed - whether it was processed by the Issuer or by STIP. DMSA also does not know if the original was approved or declined. Hence, if STIP cannot process a reversal, it returns response code 21 to indicate that no action was taken.

**Note** Issuers are not required to respond to reversal messages with response code 00 (successful approval/completion or that PIN Verification by VEAS is valid) in field 39 - Response Code.

#### 8.13.1.1 Activity testing on reversals

VEAS performs Positive Cardholder Authorization Service (PCAS) activity testing in STIP for reversals as follows.

Unlike processing for originals, VEAS does not test reversal activity against pre-set Issuer activity limits. For a reversal, VEAS tries to ensure that a prior original containing a Cardholder billing amount equal to that in the reversal (partial or full) is present in the Cardholder Database (CDB). VEAS checks the CDB for originals containing amounts greater than or equal to the reversal's Cardholder billing amount.

During STIP reversal processing, VEAS can find previous activity in the CDB only if the original (with the same or greater Cardholder billing amount) was approved in the same day in STIP (and therefore that day's STIP activity is saved in the CDB). If the original had been approved by the Issuer, it would not have received STIP activity testing, and its STIP activity would not have been saved in the CDB.

When VEAS can determine that the reversal's corresponding original activity is present in the CDB, VEAS prepares to respond with response code 00 (reversal approved - original located in CDB). For ATM reversals, VEAS also subtracts the Cardholder billing amount, in USD, from the CDB.

**Note** Partial reversals do not apply to ATM Transactions.

When VEAS cannot determine that the reversal's corresponding original activity is present in the CDB, VEAS prepares to respond with response code 21 (reversal approved - original not located in CDB), indicating that VEAS has successfully reversed the transaction but was unable to determine that there had been a corresponding prior authorization original.

Functionally, a response code of 00 or 21 has no difference in VEAS processing or transaction settlement. VEAS does evaluate the PCAS reversal activity testing response codes against response codes from other STIP services, and selects the most severe response code for responding to the Acquirer.

### 8.13.2 Money transfer Original Credits in STIP

Visa has implemented the ability for non-US Issuers to use STIP processing for money transfer OCTs. When a money transfer OCT is processed in STIP, an 0120 STIP advice or an 0220 STIP advice is sent to the Issuer.

#### 8.13.2.1 STIP parameters for money transfer OCTs

Table 32 shows the STIP parameters used for money transfer OCTs.

**Table 32: STIP parameters for money transfer OCTs**

| STIP parameters for money transfer OCTs | |
|---|---|
| **STIP parameter** | **Description** |
| Issuer Limit | This is the maximum USD amount that Visa can approve on behalf of the Issuer for a transaction when the Issuer is available.<br>If the Issuer is not available, the Issuer limit is ignored.<br>The default value for the Issuer limit is zero. To activate STIP processing for money transfer OCTs, the Issuer limit must be changed to an amount between USD 1.00 and USD 2,500.00.<br>**Important** The Issuer limit is separate from the existing edit in DMSA, VEAS and DMSC that limits all money transfer OCTs to a maximum of USD 2,500.00. This edit is not changed. |
| 1-Day Amount | This is the maximum accumulated USD amount for a single day that Visa Europe can approve on behalf of the Issuer.<br>There are separate limits for when the Issuer is available, and when the Issuer is not available.<br>This amount does not include any transactions approved by the Issuer.<br>The default value for the 1-day amount is USD 65,500. |
| 1-Day Count | This is the maximum number of transactions in a single day that Visa Europe can approve on behalf of the Issuer for an account.<br>There are separate limits for when the Issuer is available, and when the Issuer is not available.<br>This number does not include any transactions approved by the Issuer.<br>The default value for the 1-day count will be 250. |
| 4-Day Multiplier | This is the multiplier value that is used with the 1-day amount and 1-day count to determine the maximum Transaction Amount and count within a four-day period that Visa Europe can approve on behalf of the Issuer for an account.<br>There are separate multiplier values for when the Issuer is available, and when the Issuer is not available.<br>The 4-day multiplier applies to transactions for the current day and preceding three days.<br>The default value for the 4-day multiplier is 4.00.<br>For money transfer OCTs, the 1-day amount times the 4-day multiplier must be at least USD 2,500.00. |

### 8.13.2.2 STIP processing business rules for money transfer OCTs

Visa has implemented the STIP processing rules shown in Table 33 for money transfer OCTs.

**Table 33: STIP processing business rules for money transfer OCTs**

| STIP processing business rules for money transfer OCTs | |
|---|---|
| **Condition** | **Business rule** |
| The Transaction Amount is greater than the Issuer limit. | This limit is only used when the Issuer is available. Transactions above this limit are forwarded to the Issuer, and transactions below this limit are further reviewed to determine if Visa Europe can process the transaction in STIP or forward the transaction to the Issuer. |
| For an account, the total amount of all money transfer OCTs that Visa Europe has approved on behalf of the Issuer for the current day plus the current transaction is greater than the 1-day amount. | Visa Europe attempts to send the authorization to the Issuer for approval. If the Issuer is unavailable, the transaction is declined with the response code 61 (exceeds approval amount limit). |
| For an account, the total number of all money transfer OCTs that Visa Europe has approved on behalf of the Issuer for the current day plus the current transaction is greater than the 1-day count. | Visa Europe attempts to send the authorization to the Issuer for approval. If the Issuer is unavailable, the transaction is declined with the response code 65 (exceeds withdrawal frequency limit). |
| For an account, the total amount of all money transfer OCTs that Visa Europe has approved on behalf of the Issuer for the current day and preceding three days plus the current transaction is greater than the 1-day amount times the 4-day multiplier. | Visa Europe attempts to send the authorization to the Issuer for approval. If the Issuer is unavailable, the transaction is declined with the response code value of 61. |
| For an account, if the total number of all money transfer OCTs that Visa Europe has approved on behalf of the Issuer for the current day and preceding three days plus the current transaction is greater than the 1-day count times the 4-day multiplier. | Visa Europe attempts to send the authorization to the Issuer for approval. If the Issuer is unavailable, the transaction is declined with the response code value of 65. |

### 8.13.2.3 Money transfer business rules: business application identifier AA or PP

When a money transfer 0100 Authorization Request and 0200 Full financial messages with a business application identifier value of AA or PP is received, the following business rules apply:

**Table 34: Money transfer business rules: business application identifier AA or PP**

| Money transfer business rules: business application identifier AA or PP | |
|---|---|
| **Condition** | **Business rule** |
| An Original Credit 0100 Authorization Request is sent by a US Acquirer or originator. | VEAS declines the transaction with the response code 93 (transaction cannot be completed). |

| Money transfer business rules: business application identifier AA or PP | |
|---|---|
| **Condition** | **Business rule** |
| An Original Credit is received with an MCC in field 18 - Merchant Type that is not 4829 (Wire transfer money orders) or 6012 (Financial institutions merchandise and services). | VEAS rejects the transaction with the reject code 0635 (invalid Merchant Category Code (MCC) for EPS or NSR transaction). |
| An Original Credit 0100 Authorization Request is sent to a US Issuer. | VEAS declines the transaction with the response code value of 93. |
| The value of field 4 - Amount, Transaction is greater than USD 2,500.00. | VEAS declines the transaction with the response code 61 (exceeds approved amount limit). |
| The recipient's Issuer does not support field 104 in TLV format. | VEAS declines the transaction with the response code value of 57. |
| Field 104, dataset ID 5F is not present in an Original Credit transaction. | VEAS rejects the transaction with the reject code 0494 (field or data missing). |
| Field 104, dataset ID 71 is not present in an Original Credit transaction. | VEAS rejects the transaction with the reject code 0494 (field or data missing). |
| For an Original Credit message, neither the Sender Reference Number in tag 01, nor the Sender Account Number in tag 02, is present in field 104, dataset ID 5F.<br>**Note** Either the Sender Reference Number tag, or the Sender Account Number tag, or both, must be present in money transfer Original Credit messages. | VEAS declines the transaction with the response code64 (transaction does not fulfil AML requirement). |
| For an Original Credit message, when the Acquirer or originator and recipient's Issuer are in different countries, and one or more of the following tags are not present in field 104, dataset ID 5F:<br>■ Sender Name in tag 03<br>■ Sender Address in tag 04<br>■ Sender City in tag 05<br>■ Sender State in tag 06 (required when the Sender Country in tag 07 contains a value of US or CA)<br>■ Sender Country in tag 07 | VEAS declines the transaction with the response code value of 64. |
| The total number of all Original Credit transactions submitted within a four-day period for the account exceeds the maximum number set by the recipient's Issuer. | VEAS declines the transaction with the response code 65 (exceeds withdrawal frequency limit).<br>This business rule is specific to Original Credit transactions, and is not part of PCAS. |
| The total amount of all Original Credit transactions submitted within a four-day period for the account exceeds the maximum amount set by the recipient's Issuer. | VEAS declines the transaction with the response code 61 (exceeds approval amount limit). |

| Money transfer business rules: business application identifier AA or PP | |
|---|---|
| **Condition** | **Business rule** |
| The Issuer is not available for an Original Credit transaction. | VEAS declines the transaction with the response code 91 (Issuer unavailable). |
| A duplicate transaction is received. | VEAS rejects the transaction with the response code 94 (duplicate transmission). |

When DMSA or SMS receives an Original Credit 0100 or 0200 Request message with a business application identifier value of AA or PP, if the recipient's Issuer does not participate in Visa Money Transfer transactions, DMSA or SMS overlays the value of the business application identifier as follows before forwarding the request message to the Issuer:

- BI when field 18 contains an MCC value of 6012
- MI when field 18 contains an MCC value of 4829

# 9 Non-authorization messages

## 9.1 Online file maintenance request (0302) and response (0312) message flows

Issuers can use online file maintenance messages to maintain their files stored in system files. There are two types of file maintenance messages:

- **File Update**: Members use file updates to add, to change, or to delete information in a file
- **File Inquiry**: Members use file inquiries to request data from a file

DMSA sends a response to an update request acknowledging a successful update or providing an error reason code that explains why it could not perform the update. The response to a file inquiry request contains the requested record or contains an error reason code explaining why the record could not be provided.

Issuers are responsible for creating and for maintaining the information in several of the files in the CDB. Issuers use online file maintenance messages to update files and to request individual records in any of their files.

Issuers can update the:

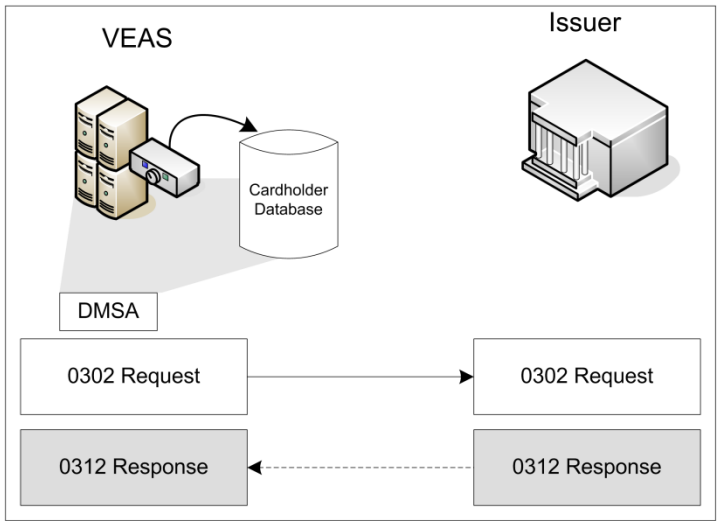
- Exception File
- PIN Verification File
- Risk-Level File

VEAS can automatically update files in the Cardholder Database for participants in the Automatic Cardholder Database Update (Auto-CDB) Service, the Chargeback Reduction Service (CRS). Participants receive 0120 or 0322 file update advices when VEAS updates the Exception File on their behalf.

See Appendix A, *Cardholder Database and Advice Files*, for more information.

Figure 25 illustrates the file maintenance message flow for Issuers.

**Figure 25: File maintenance message flow for Issuers**



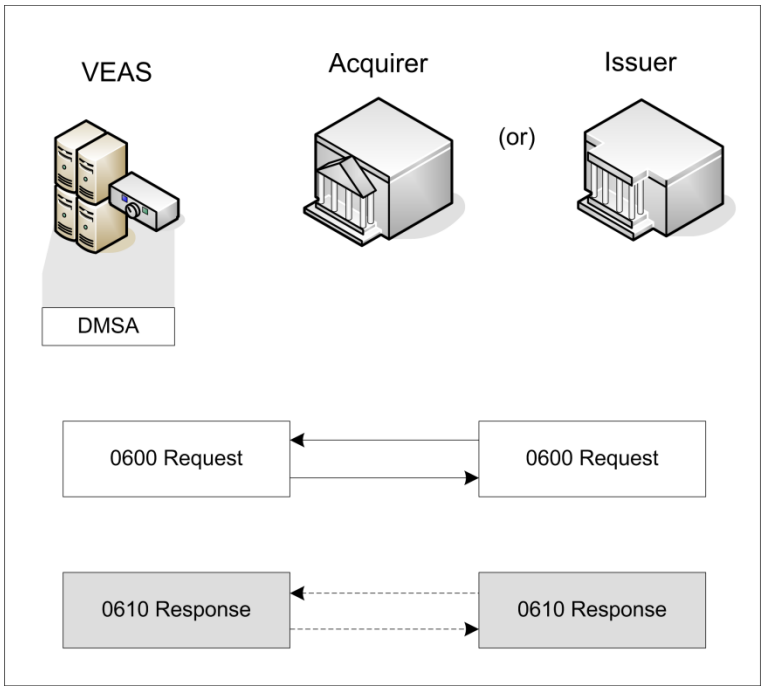
## 9.2 Administrative request (0600), response (0610), and advice (0620) message flows

DMSA, Acquirers, and Issuers can initiate administrative 0600 requests. DMSA sends 0600 administrative messages and 0620 advices to provide information or warnings to Members.

Administrative messages contain free text rather than codes. Members can route them to an offline device such as a printer for hardcopy printout for manual evaluation. Members do not respond to administrative messages.

Figure 26 illustrates the administrative message flow.

**Figure 26: Administrative message flow**




## 9.3 Network management request (0800) and response (0810) message flows

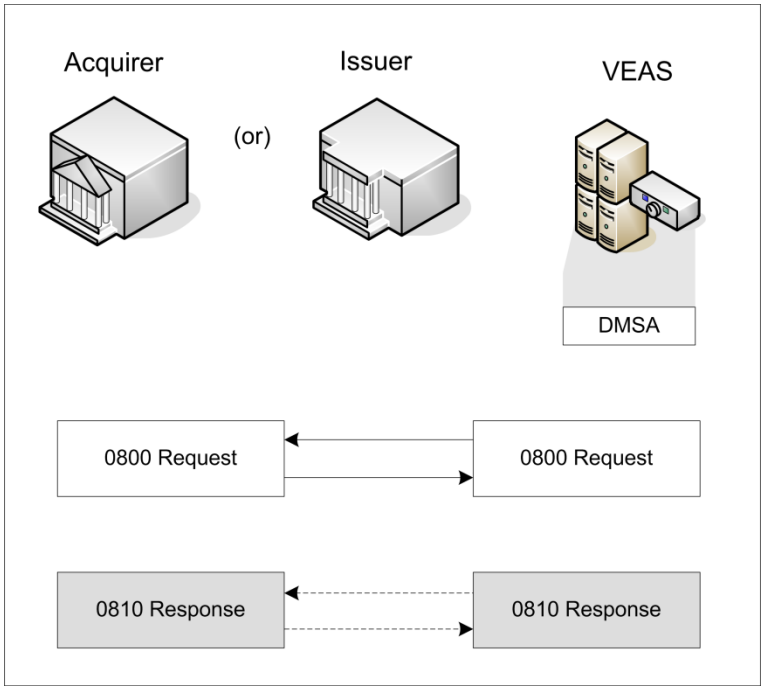
DMSA uses network management messages for DMSA network management functions that control access to the Visa Europe System, and message traffic. Network management functions include monitoring the operating status of Processing Centres.

The Member operating events or conditions that DMSA monitors include:

- Network sign-on
- Test mode
- Advice Recovery mode

Figure 27 illustrates the network management message flow for network sign-on mode and for test mode.

**Figure 27: Network management message flow**




## 9.4 Network sign-on

DMSA uses 0800 and 0810 network management messages to communicate system status information between the Visa Europe System and Members, and to initiate failure-recovery activities:

**Sign-On**: Issuers and Acquirers use sign-on messages to notify DMSA that they are available to send and receive messages. Sign-on messages contain a value of 071 in field 70 - Network Management Information Code that indicates that the centre has begun processing.

**Sign-Off**: Issuers and Acquirers use sign-off messages to notify DMSA that they are unavailable to send and receive messages. Sign-off messages contain a value of 072 in field 70 that indicates that the centre has stopped processing.

**Important** To recover from Sign-Off mode, Visa Europe recommends that Members sign their stations off from DMSA before they shut down their systems and sign on their stations to DMSA again to resume processing Authorization Requests.

## 9.5 Test echo message

Members that process DMSA and SMS messages using a common computer interface can also use 0800 network management request messages to test network communications. Processing Centres insert a value of 301 in field 70 to test communications. VEAS uses the same messages to test network communications with Processing Centres as well. If the VEAS request is a communications test, the recipient must acknowledge the request with an 0810 response message.

VEAS initiates test messages to Members through their Visa Europe System connections during periods of inactivity to verify the Members' connections. The frequency of the echo test messages are:

- **DMSA**: Once per minute
- **SMS**: Once every five minutes

SMS Members can also choose to have VEAS send echo test messages at least once every five minutes regardless of traffic conditions whenever they are connected to the Visa Europe System.

## 9.6 Advice recovery mode

Issuers can use 0800 network management messages to recover advices from the advice file. Issuer stations can sign themselves on to DMSA in Advice Recovery mode anytime by sending a network management message (0800) to DMSA.

When an Issuer station is in Advice Recovery mode, it can recover advices in one of the following ways:

- The station can recover advices automatically every two seconds without a required response. Usually advices arrive in chronological order, but the advices created at the secondary VIC may affect the order. The station requests the automatic method by sending DMSA an 0800 message with network code 078.
- The station can choose a more rapid advice-recovery process by prompting DMSA to send the next advice. To initiate rapid advice recovery, the station sends an 0800 message with a value of 066 in field 70, requesting DMSA to send the next advice. If the next prompt is longer than two seconds, normal pacing of transmission resumes.

  **Note** Stations can also recover advices through the DMSC System rather than by using online messages. For information about DMSC advices, refer to DMSC documentation.

Processors can sign on more than one station to advice recovery. DMSA performs advice delivery to each station once every two seconds. DMSA delivers advices from each separate BIN queue as evenly as possible.

DMSA stores advices in the advice file for a maximum of 15 days. If Issuers do not recover their advices within 15 days, DMSA purges them from the file. Each BIN has its own advice queue, and there is no limit to the number of advices a queue can contain. Issuers may retrieve advices until a queue is empty, but they cannot delete advice queues unless they delete the BIN. Issuers cannot transfer advices in a given queue to another queue. Issuers can retrieve advices only once.

Additionally, Issuers can choose to remain in Advice Recovery mode after their advice files are empty so they can recover advices as DMSA creates them. Advice recovery does not interrupt authorization traffic.

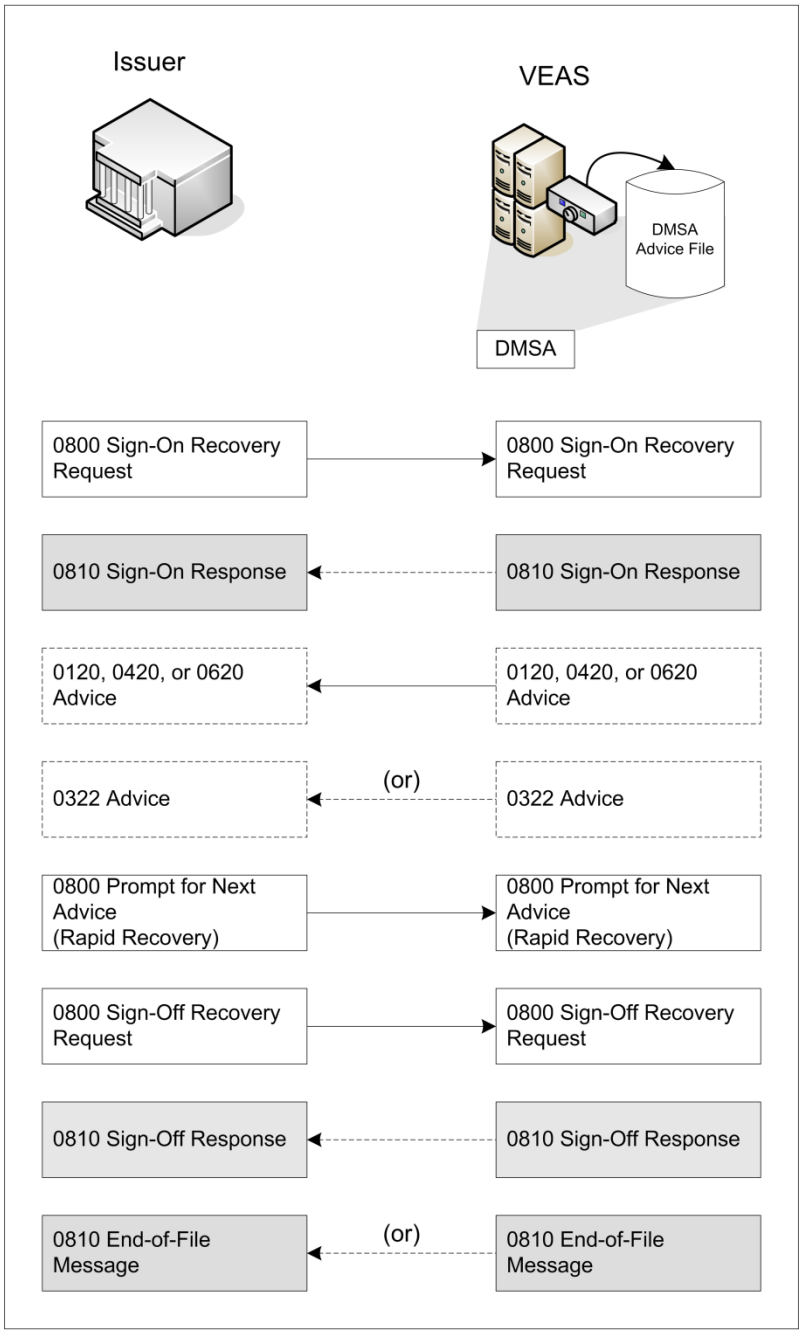
Processors send advice recovery sign-off messages to indicate that they do not want to receive DMSA-generated advice messages. Centres insert the value 079 in field 70.

Issuers can recover advices even if they are signed off from Authorization Request traffic. During these periods, STIP processes requests that would normally be delivered to the Issuer. To resume processing Authorization Requests, the Processing Centre uses the normal

procedure to sign on again. For a description of the service and its support for advice recovery, refer to the information about the DMSA Advice Retrieval Service in the *Visa Europe Technical Service Descriptions*.

Figure 28 illustrates the network management message flow for advice-recovery requests.

**Figure 28: Advice recovery message flow**



# A Cardholder Database and Advice Files

The Cardholder Database (CDB) and the Advice File reside at each Visa Interchange Center (VIC). VEAS is responsible for ensuring the integrity of all system files. To manage information in the files, VEAS accepts a file update only from the Issuer responsible for the set of Card numbers in the message.

VEAS backs up all of the system files periodically so they can be recovered in the event of a system failure. The system also ensures that the copies of the files at each of the VICs are correct and are synchronized.

The Visa Europe System no longer allows the use of format 1 file maintenance messages. Members must use format 2 for file maintenance messages. Format 2 provides Members with enhanced file maintenance capability, and Members can use format 2 to maintain all of the files in the Cardholder Database.

## A.1 Overview of Cardholder Database files

The DMSA CDB contains Cardholder information that stand-in processing (STIP) uses to authorize transactions and to verify accounts, addresses, and PINs. The CDB also contains Positive Cardholder Authorization Service (PCAS) limits for individual Cardholders.

The Cardholder Database contains the following files:

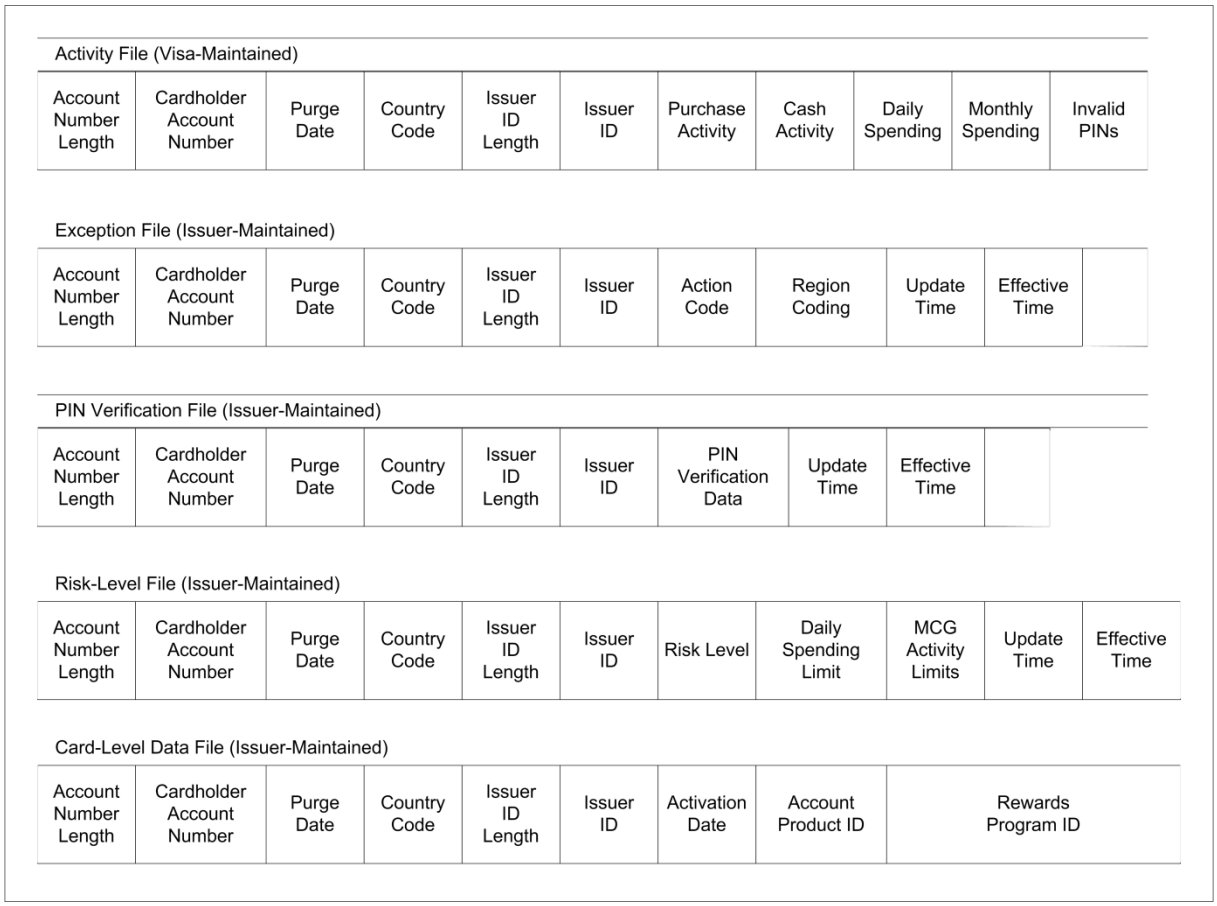
- Activity File
- Exception File
- PIN Verification File
- Risk-Level File
- Card-Level Data File
- Advice File

Visa Europe is responsible for maintaining the activity (and advice) files; Issuers are responsible for establishing and for maintaining the rest.

### A.1.1 Database content

Figure 29 shows the layout for each file in the Cardholder Database.

**Figure 29: Layout of Cardholder Database files**




## A.1.2 File record formats and update methods

Table 35 lists the file types for the Cardholder Database files.

**Table 35: File record formats and update methods**

| File record formats and update methods | | |
|---|---|---|
| **File** | **Format** | **Name/Type** |
| DMSA Cardholder ID: PIN Verification data and address verification data | Format 2 | C2 |
| Exception File (Issuer institution ID and country code fields are not applicable) | Format 2 | E1 |
| Exception File | Format 2 | E2 |
| PIN Verification File | Format 2 | P2 |
| Risk-Level File | Format 2 | R2 |
| Card-Level Product ID | Format 2 | n/a |

See the end of this appendix for additional information about online file updating.

## A.1.3 Fields common to all Issuer-maintained CDB files

Table 36 lists the fields common to all of the Issuer-maintained CDB files. The individual file sections do not repeat their descriptions.

**Table 36: Fields common to all Issuer-maintained CDB files**

| Fields common to all Issuer-maintained CDB files | |
|---|---|
| **Field** | **Purpose** |
| Account Number Length | This field defines the number of digits in the Account Number and is required in every record. |
| Cardholder Account Number | This field identifies the Cardholder account or relationship. The following Account Number types are valid:<br>■ 13- or 16-digit numeric Card numbers<br>■ 5-28-digit numeric Card numbers and Proprietary Card numbers<br>■ 5-15-character alphanumeric private-label Card numbers |
| Purge Date | The purge date is the approximate time that the record is removed from the file. The purge date format is the 6-digit date (YYMMDD).<br>VEAS determines purge date centuries as follows:<br>■ If YY = 00-49, then the century is the 21st (years 2000 through 2999)<br>■ If YY = 50-99, then the century is the 20th (years 1900 through 1999)<br>**Note** VEAS rejects Exception File records submitted with purge date years 2042 through 2098.<br>See the individual Cardholder Database file descriptions in this appendix for further file-specific purge date information. |
| Country Code | This field identifies the country of the Card Issuer and is required if either the Account Number or the Issuer ID is non-ISO standard. VEAS uses this field, along with the Issuer institution ID field, to identify the Issuer. |
| Issuer Institution ID Length | This field defines the number of digits in the Issuer institution ID and is required only when the Account Number does not comply with the ISO standard. |
| Issuer Institution ID | This field identifies the Issuer when VEAS cannot determine it from the Account Number of the Cardholder. VEAS requires this field for Proprietary Card and private-label Card numbers if the account range duplicates that of another Issuer's accounts. VEAS uses the field with the country code field to identify the Issuer Processor. Issuers must prearrange with Visa Europe the assignment of an ID. Issuers cannot use the Issuer institution ID with Visa or MasterCard accounts. They can only use it with Account Numbers that do not comply with the ISO standard. |

| Fields common to all Issuer-maintained CDB files | |
|---|---|
| **Field** | **Purpose** |
| Update Time | Update time is a system-generated time stamp indicating the date and time that the Visa Europe System establishes a record. Update time is not visible to users but is available to Visa Europe staff for research and for settling Chargeback disputes. VEAS automatically generates the update time when it first enters a negative (decline or referral) or a pick-up record in the file, and when it changes a VIP (Very Important Person) or XA code in an existing record to a negative or pick-up code.<br>For the Exception File, update time refers to the first date and time VEAS updates the file with a pick-up code that is, non-approval codes 01, 04, 07, 41, or 43. VEAS keeps this date and time and does not change it during subsequent updates as long as the action code is a pick-up code. For file types other than the Exception File, the update time indicates the date and time of the last record update. |
| Effective Time | The effective time is the date and time that the VIC receives the message. This time applies both to adding records and to deleting records. |

The following sections describe the individual files within the Cardholder Database.

## A.2 Activity File

### A.2.1 File description

The Activity File contains accumulated transaction and PIN activity processed at the VIC for each Cardholder. It does not contain individual transaction activity.

STIP uses the file when performing activity checks as part of authorization processing; it accumulates activity for approved transactions. The PIN Verification Service (PVS) uses the file to store the number of invalid PIN-entry attempts.

Issuer Processors specify whether STIP is to check activity and define the activity limits STIP is to use in the calculation. Issuers' activity limits reside in the system tables. The activity limit formula comprises the following three calculations:

- The number of times a Cardholder can use his or her Card in one day (count)
- The maximum amount allowed for each occurrence during that same day (amount)
- A 4-day multiplier value between 1 and 4 that STIP uses to establish the count and amount limit totals over a four-day period (current day plus three days)

Accumulated transaction activity represents running count and amount totals, which STIP uses to determine if a current transaction remains within the Issuer's allowable limits or exceeds them. The PIN-entry retry activity limit is an Issuer-defined value that directs STIP to decline transactions when consecutive PIN-entry attempts exceed the established threshold.

### A.2.2 File content

The Activity File organises records by Account Number of the Cardholder. Each Cardholder record contains accumulators for:

- Merchant group activity

- Invalid PIN-entry activity

Figure 30 illustrates the basic structure of an Activity File record.

**Figure 30: Activity File record layout**

| Activity Record | | | | |
|---|---|---|---|---|
| Purchase Activity | Cash Activity | Daily Spending | Monthly Spending | Invalid PINs |

## A.2.3 Unique fields

The following subsections describe the fields unique to the Activity File and their uses.

### A.2.3.1 Purchase and cash Merchant group activity

Activity File records contain accumulated Merchant Category Group (MCG) activity counts and amounts for STIP-approved purchase and cash transactions.

Issuers establish activity limits in sets comprising a count, an amount, and a 4-day multiplier. Visa Europe requires activity limits at a minimum for Total Purchase and Total Cash categories. Issuers also can establish activity limit sets for one or more different purchase or cash MCGs, daily spending, monthly spending, and invalid PINs.

The purchase activity portion of the activity record is divided into the purchase MCGs. Activity accumulation includes approvals both for Issuer-available conditions and for Issuer-unavailable conditions for each MCG. The Visa Europe System does not maintain separate Issuer-available counts and Issuer-unavailable counts.

Table 37 illustrates the relationship between activity records and MCGs.

**Table 37: Activity record layout - purchase activity MCG breakdown**

| **Activity record layout - purchase activity MCG breakdown** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Purchase activity by MCG** | | | | | | | |
| | Commercial Travel | Lodging | Auto Rental | Restaurant | MOTO/e-commerce | Risky Purchase | Total Purchase |
| 1-Day Amount Totals | | | | | | | |
| 1-Day Count Totals | | | | | | | |
| 4-Day Amount Totals | | | | | | | |
| 4-Day Count Totals | | | | | | | |

As shown in Table 38, the cash activity portion of the activity record is divided into two cash MCGs.

**Table 38: Activity record layout - cash activity MCG breakdown**

| Activity record layout - cash activity MCG breakdown | | |
|---|---|---|
| **Cash activity by MCG** | | |
| | Total Cash | ATM Cash |
| 1-Day Amount Totals | | |
| 1-Day Count Totals | | |
| 4-Day Amount Totals | | |
| 4-Day Count Totals | | |

### A.2.3.2 PIN-entry retry activity data

For PIN Verification Service (PVS) participants, the activity record contains one accumulator that tracks the number of consecutive invalid PIN entries for the current day, as illustrated in Figure 31. When the number of attempts equals the Issuer-specified PIN-entry retry limit, STIP declines the transactions (but does not request pick-ups). VEAS resets the invalid PIN accumulator to zero at 00:00 hours.

**Figure 31: Activity Record Layout - Invalid PIN breakdown**

| Invalid PINs |
|---|
| Number of consecutive invalid PIN entries today |

Some Members have reciprocal agreements to pick up the Cards after the specified number of invalid PIN-entry attempts occurs.

## A.2.4 Maintenance and update

Once a day, at 00:00 hours GMT, the Visa Europe System updates the Activity File by **rolling over** transaction accumulators so that the file always reflects four days of current activity.

The Visa Europe System clears invalid PIN counts daily. Also, as long as invalid PIN-entry activity is under the limits, the Visa Europe System clears the PIN counts each time the VIC receives a valid PIN. The Activity File clears the counts to reflect only consecutive invalid PIN-entry attempts rather than all attempts to enter a PIN. For further information about excessive PIN-entry attempt processing, refer to the description of the PIN Verification Service (PVS) in the *Visa Europe Technical Service Descriptions*.

## A.2.5 Purging records

Members do not purge records from the Activity File. The Visa Europe System performs this task.

## A.3 Exception File

### A.3.1 File description

The Exception File is a VIC-resident, online file containing Cardholder account records. VEAS accesses the file during STIP processing. Reasons for Exception File-based responses include:

- VEAS should always deny authorization for the account
- The Merchant or Member should confiscate the Card if presented
- The response should be a referral

  The Acquirer Processor should contact the Issuer Processor directly to obtain authorization. In the US region, Acquirer Processors should call the International Automated Referral Service (IARS).
- The Issuer Processor should process the request when possible
- VEAS should approve transactions on this account regardless of Cardholder activity
- To prevent Cards from being used in certain countries

VEAS uses the Exception File for processing authorizations. Issuers maintain the file. If Issuers want to list accounts in the Card Recovery Bulletin (CRB), the listings must reside in the Exception File.

Issuers can update the Exception File using a single transaction, message type 0302, with file type E3 specified in field 101 - File Name. Messages must be in V.I.P. message format for E3 updates. If an Account Number is listed using file type E3, all subsequent updates for that Account Number must use file type E3; otherwise, VEAS rejects the update.

The Exception File is the source for the Card Recovery Bulletin (CRB). Entering the Account Number in the Exception File with a pick-up response code and the CRB region coding ensures that the Account Number is included in the applicable bulletins. See Appendix A.3.3.2, *Region codes*, for specific region codes.

**Note** International CRBs contain only accounts with pick-up action codes, that is, 04 (pick up Card, unspecified, non-fraudulent), 07 (pick up Card, special conditions other than lost, stolen, or counterfeit Card), 41 (pick up Card, lost Card [fraud]), or 43 (pick up Card, stolen Card [fraud]).

#### A.3.1.1 Generating Visa Card Recovery Bulletins (CRBs)

DMSA extracts data from the Exception File for the Card Recovery Bulletin (CRB) Service to create CRBs. Issuers can list Visa Account Numbers in the Exception File, coded to appear in specified bulletins and files so Merchants can pick up the Cards.

Issuers submit updates to the Exception File:

- Online through:
  - Online file maintenance messages, or
  - The Automated Cardholder Database Update (Auto-CDB) Service
- Offline through:
  - Their Visa Resolve Online (VROL) connection, or
  - Batch tape, or
  - GCAS

The CRB Service combines the Exception File records with counterfeit Card accounts and blocked BINs to produce the pick-up file. Visa distributes the sorted pick-up list through electronic bulletins and files.

Issuers can delete Exception File records from blocked BINs if the Account Number range in which the deletion falls is still pointing to one of the Member's current Processing Centre Records (PCR).

For information about the CRB Service refer to the *Visa Europe Technical Service Descriptions*, and for information about the Auto-CDB Service refer *to System Management for Members*.

### A.3.2 File content

The Exception File contains records organised by Account Number, as illustrated in Figure 32. VEAS generates the update time, the effective time, the service indicators, and the history indicators.

**Figure 32: Exception File record layout**

| Account Number Length | Cardholder Account Number | Purge Date | Country Code | Issuer ID Length | Issuer ID | Action Code | Region Coding | Update Time | Effective Time |
|---|---|---|---|---|---|---|---|---|---|

### A.3.3 Unique fields

The following subsections describe the unique Exception File fields.

#### A.3.3.1 Action codes

Each Exception File record must contain one of the action codes for field 127 - File Maintenance listed in Table 39 and Table 40. For more information about this field and about valid action codes, refer to the *DMSA Technical Specifications*.

**Table 39: Exception File action codes-a**

| Exception File action codes-a | |
|---|---|
| **Code** | **Definition** |
| 01 | Refer to Issuer of the Card |
| 04 | Pick up Card |
| 05 | Do not honour<br>**Note** This negative response code only causes US-domestic accounts to be listed in CRBs. Issuers in all other regions do not use this response code if they want the account listed in CRBs. |
| 07 | Pick up Card, special condition |
| 11 | Approval for VIP (Very Important Person) |
| 41 | Lost Card, pick up |
| 43 | Stolen Card, pick up |

Action codes A1 through A9 are VIP codes associated with special high-value activity limits. Amount limits are in USD.

**Table 40: Exception File action codes-b**

| Exception File action codes-b | | | | |
|---|---|---|---|---|
| **Code** | **One-day limits** | | **Four-day limits** | |
| | **Amount** | **Count** | **Amount** | **Count** |
| A1 | USD 1,500 | 3 | USD 1,500 | 9 |
| A2 | USD 2,000 | 5 | USD 3,500 | 12 |
| A3 | USD 3,000 | 8 | USD 6,000 | 14 |
| A4 | USD 4,500 | 12 | USD 8,000 | 25 |
| A5 | USD 6,000 | 15 | USD 10,000 | 40 |
| A6 | USD 8,000 | 20 | USD 14,000 | 50 |
| A7 | USD 10,000 | 25 | USD 20,000 | 100 |
| A8 | USD 1,500 | 4 | USD 2,000 | 10 |
| A9 | USD 2,225 | 6 | USD 3,500 | 13 |
| XA | Forward to Issuer; default to 00 | | | |
| XD | Forward to Issuer; default to 05 | | | |

The field 127 codes are valid for file updates. The action codes specify how STIP is to respond when it processes requests on the listed account. These action codes appear in Authorization Responses and in related advices as field 39 response codes. The Visa Europe System allows only one action code per record.

VEAS uses applicable mandatory and Issuer-specified amount limits to determine whether to route a transaction to an available Issuer. Action code 11 does not trigger a referral if VEAS routes the transaction to STIP.

### A.3.3.2 Region codes

Each Exception File record must contain one of the region codes for field 127 listed in Table 41. For information about this field and valid action codes, refer to the *DMSA Technical Specifications*.

**Table 41: DMSA CRB region codes**

| DMSA CRB region codes | |
|---|---|
| **Region code** | **Geographic area** |
| 0 | Do not list in any Card Recovery Bulletin |
| A | All countries in the Asia-Pacific (AP) region |
| B | Africa and part of the Middle East (includes countries that are part of Visa sub-regions 3 and 5 of the Central Europe, Middle East, and Africa region (CEMEA)) |
| C | All Visa Canada |
| D | National CRB indicator |
| E | Visa Europe and part of the Middle East (includes countries in the Central Europe, Middle East, and Africa (CEMEA) region not classified as part of CRB region B) |

| DMSA CRB region codes | |
|---|---|
| **Region code** | **Geographic area** |
| F | All countries in the Latin America and Caribbean (LAC) region |
| Y | All non-US CRB regions (regions A, B, C, E, F) |
| Z | All CRB regions |

Issuers use region codes to specify the geographical areas in which they want the Account Number of the Cardholder to be published for pick-up in the Card Recovery Bulletin (CRB) Service files and bulletins. All exception records that contain pick-up response codes require region coding.

Issuers fill this field with spaces in non-pick-up records.

Issuers can suppress the publishing of pick-up Account Numbers by using region code 0, which means to exclude the account from RCRFs (the electronic versions of pick-up listings available to non-US users). However, the CRB Service includes region 0 accounts in the NCRF (the electronic version of pick-up listings available to US Member Processors).

Issuers use region code E to include the account in the Visa Europe CRB. Issuers use region code E for all electronic STIP authorizations regardless of the region in which the Acquirer Processor or the Issuer Processor is located.

Issuers can place any combination of region codes in field 127 in any order and with or without embedded spaces, except that they cannot specify another region code in combination with region code 0. The Visa Europe System includes an Exception File record with region code 0 in the NCRF, but not in RCRFs.

For complete details about region coding and about other CRB considerations, refer to the description of the Card Recovery Bulletin (CRB) Service in the *Visa Europe Technical Service Descriptions*, and the *Card Recovery Bulletin Service User's Guide*.

### A.3.4 Maintenance and update

Issuers can view their exception records using:

- Online requests
- Exception File report subscriptions in electronic or printed form
- Exception File raw data file subscriptions
- Visa Resolve Online (VROL)

The following subsections explain these options.

#### A.3.4.1 Visa Europe System connection

Issuers equipped with a Visa Europe System connection can use online messages to review a Cardholder's exception record. The system displays the Issuer-maintained fields; it does not display all of the fields maintained by the Visa Europe System, such as the effective time field.

Issuer Processors can request a record at any time while signed on to the network, although the Visa Europe System may restrict file access to low-volume hours. Issuer Processors must be authorized to access the file. For programming details, refer to the description of file inquiry message type 0302 in the *DMSA Technical Specifications*.

### Online Exception File editing summary (0302 messages)

Members can maintain their exception records without knowing the current status of the record on the VEAS files.

- VEAS accepts attempts to add a record for a Cardholder that is already on the file as changes
- VEAS accepts attempts to change a record for a Cardholder that is not already on the file as additions
- VEAS rejects attempts to delete a record that is not on the file with error code 565 (no record on file)
- VEAS processes attempts to add, change, or delete exception records that are subject to a dual-item check according to Member instructions (add, change, or delete)

  **Note** An out-of-synchronisation condition does not affect the update task.

Which file types Issuers can use depends on the sending station.

DMSA Members must use E3 and E4 CMI Exception File types unless the station is associated with a PCR that is also allowed to use file types E1 and E2. Violations result in reject code 530 (invalid file type).

Table 42 summarises the Exception File update processing actions.

**Table 42: Exception File update processing actions**

| Exception File update processing actions | | |
|---|---|---|
| **Action/file type** | **Card number valid<br>Not present on file result** | **Card number valid<br>Present on file result** |
| Add E1 | | Replace |
| Add E2 | | Replace |
| Change E1 | Add to File | |
| Change E2 | Add to File | |
| Delete E1 | Error - 0565 | |
| Delete E9 | Error - 0565 | |
| Add E4 | | Replace |
| Change E4 | Add to File | |

Table 43 summarises the Exception File update processing actions.

**Table 43: Exception File update processing actions**

| Exception File update processing actions | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Action / file type** | **DMSA invalid / SMS invalid** | **DMSA invalid / SMS valid** | **DMSA invalid / SMS present** | **DMSA valid / SMS valid** | **DMSA valid / SMS present** | **DMSA present / SMS valid** | **DMSA present / SMS present** |
| | **Result** | **Result** | **Result** | **Result** | **Result** | **Result** | **Result** |
| Add E3 - Network Specified | | | | | Add / Replace | Replace / Add | Replace |
| Add E3 - Network Not Specified | | | Replace | | Add / Replace | Replace / Add | Replace |
| Add E4 | | | Replace | | Replace | | Replace |
| Change E3 - Network Specified | | | | Add | Add / Change | Change / Add | |
| Change E3 – Network Not Specified | | | | Add | Add / Change | Change / Add | |
| Change E4 | | Add | | Add | | Add | Add |
| Delete E3 - Network Not Specified | 0571<br>0572 | | | | | | |
| Delete E4 | 0571<br>0572 | | | | | | |

For further information, refer to the description of the Cardholder Database in *System Management for Members*.

### A.3.4.2 Using telephone or fax machines for updates

Processing Centres of Issuers with direct network links can contact Global Customer Assistance Services (GCAS) for emergency updates during a system failure of that Processor.

The following limitations apply to telephone and fax requests:

- **US Issuer Processors**: Issuers can request manual updates for emergency purposes or for VIP accounts only. Issuers can request up to 100 updates by fax machine.
- **Non-US Issuer Processors**: Issuers can request manual VIP and emergency updates. Issuers can request up to four updates by telephone and up to 100 updates by fax machine.

The information needed for telephone, telex, or fax updating is:

1. The authorization Issuer Processor ID (4-digit Processor ID), for instance: CENTRE 4 EXCEPTION FILE
2. The country in which the Issuer Processor is located

3. The update information, grouped according to the following update transaction code:

   EA = Add

   EC = Change

   ED = Delete

   The update information is:

   - The Account Number of the Cardholder
   - The response code or forwarding code, if the request is for an addition or for a change:

     04 = Pick up Card

     05 = Decline

     07 = Pick up Card, special condition

     11 = VIP handling: use Issuer-selected limits to check Cardholder activity

     41 = Pick up Card, lost Card

     43 = Pick up Card, stolen Card

     A1-A9 = VIP handling: use special activity limits to check Cardholder activity

     XA = Forward request to centre or approve transaction

     XD = Forward request to centre or decline transaction
   - The purge date in MMDDYY format, if the request is for an addition or for a change
4. The name of the person requesting the update
5. The Processing Centre's fax or telephone number

### A.3.4.3 Automatic Cardholder Database Update (Auto-CDB) service

In addition to using 03xx file maintenance messages, Issuers can use 0110 responses if they participate in the Auto-CDB Service to insert the following file update information:

- The purge date
- The file update code 3 (delete) or 4 (replace)

  If the file update code is 4, the system converts this file information to an addition or to a change as applicable.
- The file name: E2 (Exception File)
- The action code

VEAS replaces the old Exception File information with the new information before it sends the 0110 response to the Acquirer. VEAS also creates an Issuer advice. When VEAS cannot process updates, it creates a discrepancy advice to inform the Issuer of the reason.

When the Issuer responds to an Authorization Request with a pick-up-Card response (response code 04, 07, 41, or 43), the Visa Europe System checks the Exception File to determine if it lists the Cardholder account. If the file does not list the account, the Visa Europe System automatically adds the account to the file with the applicable pick-up code and with region code 0, and includes it in the Chargeback Reduction Service. If the file lists the account with a response code other than a pick-up code, VEAS changes the listing to pick-up status.

When Cardholder Database processes were aligned, the processing of Exception File updates that Visa Europe initiates on behalf of Issuers that participate in the Auto-CDB Service changed. The following processing rules exist.

If the CDB record does not exist or is present with a non-pickup action code, Visa Europe continues to set:

- Action code to pickup
- Purge date to 60 days
- CRB region to CRB region 0

  **Note** Currently, no CRB region is set.

If the CDB record exists with a pickup action code, Visa Europe continues to extend the purge date to 60 days. Visa Europe also:

- Extends the existing CRB region listing
- If no CRB region is present, sets the CRB region to CRB region 0

Issuers may choose to receive these advice messages so they are aware of the CRB additions and extensions if they participate in the Auto-CDB Service.

VEAS only processes an update when the Authorization Response includes a valid field 39 response code and a valid field 127 file action code. Table 44 lists valid response code and file action code combinations.

### Key to Table 44

X indicates a valid combination, and the Visa Europe System forwards the Authorization Response to the Acquirer Processor (without the file update information), updates the Exception File as requested, and creates an advice of file update instead of an 0312 response.

XR indicates a valid combination for pick-up responses. Issuers cannot change a pick-up action; Issuers may change only regions and purge dates.

A blank indicates that the file update request is invalid for the Authorization Response and the Visa Europe System forwards the Authorization Response to the Acquirer Processor (without the file update information), does not update the Exception File, and creates a discrepancy advice containing error information.

**Table 44: Valid response message field combinations for Exception File updates**

| Valid response message field combinations for Exception File updates | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Authorization Response (ISO 39)** | **File action code (ISO 127, E)** | | | | | | | | **Update code (ISO 91)** | |
| | **Refer 01** | **Pick Up 04** | **Decline 05** | **Pick Up Special 07** | **Pick Up Lost Card 41** | **Pick Up Stolen 43** | **Switch to Issuer ; Approve if Unavailable XA** | **Switch to Issuer; Deny if Authorization Unavailable XD** | **Replace 4** | **Delete 3** |
| 00 Approve | | | | | | | X | | X | X |
| 01 Refer to Issuer | X | | | | | | X | X | X | X |
| 02 Refer to Issuer, Special Condition | X | | | | | | X | X | X | X |
| 04 Pick Up Card | | XR | | | | | | | X | |
| 05 Decline (US –domestic only) | X | | X | | | | | X | X | |
| 07 Pick Up Card, Special Condition | | | | XR | | | | | X | |
| 41 Pick Up Card, Lost Card | | | | | XR | | | | X | |
| 43 Pick Up Card, Stolen Card | | | | | | XR | | | X | |
| 54 Expired Card | X | | X | | | | | X | X | |
| 62 Restricted Card | X | | X | | | | | X | X | |

### A.3.4.4 Global Customer Care Services (GCCS)

When a Cardholder notifies GCCS that a Card is lost or is stolen, a service operator works online to automatically list the account in the Exception File with action pick-up code 04 and region code 0. Service staff also notify the Issuer Processor of the loss or the theft, and an advice of the Exception File update is forwarded to the Issuer Processor so the Issuer can delete or change the exception record as needed.

### A.3.4.5 Reports

VEAS produces seven Member-subscription Exception File reports:

- Report BIOSR112 - Exception File Listing
- Report BIOSR460 - Exception File Listing of Special Accounts
- Report BIOSR610 - Exception File Listing (Consolidated Report)

- Report BIOSR121 - Exception File Update Activity through Visa Terminal/Services
- Report BIOSR600 - Exception File Update Activity through Visa Terminal/Services (Consolidated Report)
- Report BIOSR450 - Exception File Update Activity (Special Accounts)

For information about these reports, refer *to SMS and DMSA Reports*.

#### A.3.4.6 Raw data files

VEAS also produces two Member-subscription Exception File raw data files:

- BIOSRUP - Exception File Update File
- BIOSRLP - Exception File Listing File

Using transaction code 33, VEAS transmits these files to the Member Processors through the DMSC System. For descriptions and samples of reports, refer to *SMS and DMSA Reports*. For information about raw data files, refer to the *DMSA Technical Specifications*.

### A.3.5 Purging records

When an Issuer initiates a replace request using an enhanced Authorization Response and the purge date is not present in the request, the system assigns the current date plus 60 days as the purge date.

#### A.3.5.1 Purge date formats

The Exception File stores only one purge date at a time for an account. This date corresponds to the expiry date of the applicable bulletin for the country in which the account is listed.

For additions and changes to Exception File records, VEAS converts the purge date to coincide with the expiry of the CRB in effect at that time, using the YYMMDD format.

If the request does not contain a purge date or contains the now invalid non-expiring purge date of 999900, VEAS converts the date to the date of the update request plus 20 years.

#### A.3.5.2 Purge date assignments

When the Auto-CDB Service initiates an update to the Exception File, the system assigns the purge date as follows:

- If the update is an addition to the Exception File, the purge date is the Transaction Date plus 60 days
- If the update is a change from non-approval status to pick-up status, the purge date is the purge date on the file or is the Transaction Date plus 60 days, whichever date is later

For more purge date considerations, refer to the *Card Recovery Bulletin Service User's Guide*.

For file update information, see Appendix A.7, *File maintenance methods*.

## A.4 PIN Verification File

### A.4.1 File description

Authorization Requests include PINs when Cardholders use them at the point-of-service or point of sale or at an ATM. Issuers or the VIC on the Issuer's behalf can verify PINs either

during normal processing or when the Issuer Processor is unavailable. The VICs use the Visa Security Module (VSM) for verification.

### A.4.2 File content

The PIN Verification File contains records organised by Account Number. Figure 33 illustrates the record layout.

**Figure 33: PIN Verification File record layout**

| Account Number Length | Cardholder Account Number | Purge Date | Country Code | Issuer ID Length | Issuer ID | PIN Verification Data | Update Time | Effective Time |
|---|---|---|---|---|---|---|---|---|
| | | | | | | PVKI PVV or IBM Offset | | |

### A.4.3 Unique fields

This section describes the unique PIN Verification File fields.

#### A.4.3.1 PIN Verification Key Index (PVKI)

For PVVs, the PIN Verification Key Index (PVKI) is a 1-digit value that points to a pair of PIN Verification Keys stored at the VIC. These keys are the same as those the Issuer uses to generate the PVV in the record. Because the Issuer can store up to six pairs of PIN Verification Keys at the VIC, the PVKI can be any value between 0 and 6. For an IBM PIN offset, the PVKI is always 4.

A 0 (zero) indicates that the PIN Verification Service (PVS) cannot verify the PIN. If the Issuer specifies that VEAS is to perform PIN Verification for a specific account range, and an individual Card has a PVKI of 0, VEAS declines transactions with PINs for that Card. When the Acquirer and the Issuer are the same entity, the PVV need not be calculated unless the Issuer chooses to do so.

#### A.4.3.2 PIN Verification Value (PVV) or IBM PIN offset

The record contains either one 4-digit PIN Verification Value (PVV) or an IBM PIN offset that is directly associated with the Account Number and the PIN. The PVV is generated by processing the Account Number, the PIN, two PIN Verification Keys, and a PVKI through Triple Data Encryption Standard (TDES) and the Visa PVV algorithm. The IBM PIN offset is generated by processing the Account Number, one PIN Verification Key, and various other inputs through TDES and an IBM PIN offset algorithm. For additional details, refer to the *Payment Technology Standards Manual*.

### A.4.4 Maintenance and update

Issuers can update accounts with 5-28-character alphanumeric Account Numbers. Refer to the *Payment Technology Standards Manual* for details about updating the PIN Verification File.

### A.4.5 Purging records

Issuers control record purging by specifying purge dates. The format for purge dates in this file is YYMMDD. VEAS converts purge dates into this format as follows:

**Purge Date**: The system does not convert Issuer-supplied 6-digit purge dates for the PIN Verification File. The 6-digit purge date of YYMMDD defaults to the last day of the month.

For information about the PIN Verification Service, refer to the *Visa Europe Technical Service Descriptions*.

## A.5 Risk-Level File

### A.5.1 File description

Issuers use the risk-level file to:

- Assign an account-specific risk level
- Assign account-specific daily spending limits
- Assign account-specific Merchant group daily activity limits

Issuers can tailor risk levels, daily spending, and activity limits for a particular Cardholder.

The file-resident risk levels override the BIN defaults and the Card-encoded risk levels. This file lists only accounts that have exceptions to the assigned default values.

### A.5.2 File content

Figure 34, Figure 35, and Figure 36 illustrate a risk-level file record. The fields in the diagram include information that identifies the Cardholder account, the Cardholder risk level, daily spending limits, and Merchant group activity limits. For daily spending and MCG activity limits, Issuers can define a different amount for periods when the Issuer is available and when it is unavailable.

The maximum limit that Issuers can specify in any one of these fields is USD 65,000.00.

**Figure 34: Risk-level file record layout**

| Account Number Length | Cardholder Account Number | Purge Date | Country Code | Issuer ID Length | Issuer ID | Risk Level | Daily Spending Limits | MCG Activity Limits | Update Time | Effective Time |
|---|---|---|---|---|---|---|---|---|---|---|

**Figure 35: Risk-level record layout - daily spending limits breakdown**

| Daily spending limits | | | |
|---|---|---|---|
| Non-cash limit | | Cash limit | |
| Issuer available | Issuer unavailable | Issuer available | Issuer unavailable |

**Figure 36: Risk-level record layout - MCG activity limits**

| MCG activity limits | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Travel | | Lodging | | Auto rental | | Restaurant | | MOTO/EC | |
| Available | Unavailable | Available | Unavailable | Available | Unavailable | Available | Unavailable | Available | Unavailable |
| | | | | | | | | | |
| Risky purchase | | Total purchase | | Total cash | | ATM cash | | | |
| Available | Unavailable | Available | Unavailable | Available | Unavailable | Available | Unavailable | | |

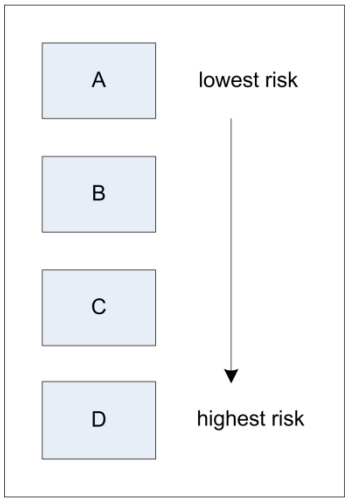
## A.5.3 Unique fields

This subsection describes the unique fields in the risk-level file.

### A.5.3.1 Risk level

Risk levels allow the Issuer to classify an individual Cardholder at one of four levels of risk, as shown in Figure 37.

**Figure 37: Cardholder risk levels**




The Visa Europe System always requires a risk-level classification when an Issuer is adding a record to the risk-level file. The VEAS default is risk level C if the Issuer has specified no other level.

### A.5.3.2 Daily spending limits

The daily spending limit is the maximum whole USD amount of cash or non-cash transactions that STIP can approve for the current day.

- Non-cash includes medical, MOTO/e-commerce, risky, and other purchase transactions

  The Visa Europe System only includes T&E Transactions in the non-cash category if separate limits do not apply.
- Cash includes ATM cash, manual cash, and Quasi-Cash Transactions

Issuers can define different limits for Issuer-available and Issuer-unavailable conditions.

#### A.5.3.3 Merchant Category Group daily activity limits

The Merchant group activity limit is the maximum whole USD amount that STIP can approve for the current day for a particular Merchant type. Issuers can define different limits for periods when the Issuer is available or is unavailable. The limits Issuers establish override the 1-day amount limits they define for the BIN. The limits do not affect transaction counts and multipliers.

For additional information about the contents of this file, refer to the *DMSA Technical Specifications*.

### A.5.4 Maintenance and update

Members establish file specifications through Visa Europe Customer Support.

### A.5.5 Purging records

Only Visa can purge records in the risk-level file.

## A.6 Card-level product ID File

### A.6.1 File description

When VEAS receives the 0100 authorization or 0200 full financial request from the Acquirer, VEAS uses the CDB data to populate field 62.23 - Card Level Results with the appropriate product value for the Cardholder before forwarding the request to the Issuer.

If the CDB does not contain information for the Account Number being processed, VEAS uses the BIN default product value. If the response code in field 39 is 00, 10, or 85 in responses, field 38 - Authorization Code, position 6, contains the value in field 62.23 (for example, B).

The Visa Incentive Network (VIN) enables Issuers to offer highly competitive rewards programs to Cardholders. For example, a Cardholder receives a 10 percent discount for purchase amounts over USD 100 at Office One. The VIN maintains the reward program requirements for programs such as Visa Traditional Rewards.

Issuers use the Card-Level Product ID File to register their reward programs and eligible Cardholders with the VIN's Cardholder Information Repository (CIR) database. In turn, the CIR periodically (daily, monthly, semi-annually) provides the online CDB with updated information needed for authorization processing. Currently, the VIN provides the CDB with Visa Traditional Rewards program data.

### A.6.2 File content

The update file consists of a control record followed by as many data records necessary for updates. A separate file containing a trailer record follows the last data record. All records (control, data, and trailer) are in variable length EBCDIC and UMF format.

**Figure 38: Card-level Product ID record layout**

| Account Number Length | Cardholder Account Number | Purge Date | Country Code | Issuer ID Length | Issuer ID | Activation Date | Account Product ID | Rewards Program ID |
|---|---|---|---|---|---|---|---|---|

The following subsections describe the fields in the records that comprise the Card-level Product ID file.

### A.6.3 Unique fields

The following fields are unique to the Card-Level Product ID File:

- Activation Date
- Account Product ID
- Rewards Program ID

#### A.6.3.1 Activation date

The 8-byte Activation Date is the date when the rewards program starts. The format is CCYYMMDD, where:

CC = last two digits of the century

YY = last two digits of the year

MM = the month

DD = the day

Activation dates can be used in multiple records for the same account with each record having a different activation date; for example, for a two-record account, record one's date is 1 September 2008, and record 2 has a date of 1 January 2009. The activation date is required when updating or replacing records. When replacing records, the activation date must be the same as the record being replaced. For new records, in which a previous record or records already exist, the new record's activation date must be more recent than the others.

VEAS adjusts the previous records' purge date if it overlaps with the new active period; that is, the previous record's purge date will match the newly added record's activation date.

#### A.6.3.2 Account product ID

The Product ID is a two-byte field. Currently, the only valid product ID is B - Visa Traditional Rewards. Refer to the description of field 62.23 in the pertinent DMSA and SMS technical specifications for a full list of product identifiers.

#### A.6.3.3 Rewards Program ID

The two-byte, six-character-maximum Rewards Program Identifier (RPIN) is required. The RPIN is assigned by Visa Registration to the Issuer participating in the Credit Rewards applicable to this account.

### A.6.4 Maintenance and update

The CDB's Card-Level Product file is updated from data in the CIR database. However, Issuers are responsible for ensuring (maintaining and updating) that the CDB file data is correct.

For further information about maintaining and updating the files in the Customer Information Repository (CIR) database, Members can contact Visa Europe Customer Support.

### A.6.5 Purging records

Issuers provide the purge dates for the file records.

## A.7 File maintenance methods

Issuers can update the Cardholder Database in any of several ways:

- Using online file update messages for individual updates
- Transmitting a batch file of updates to the VIC through a Visa Europe System connection that supports the batch file update function

Members must establish the controls necessary to ensure the accuracy of the data and the procedures for conveying updates to the VIC.

### A.7.1 Online update process summary

Issuer Processors can use an online message (0302) to add, to change, or to delete a Cardholder Database record. Members initiate update messages either through the Issuer Processor computer interface or through their Visa Europe System connection.

With 0120 and 0322 messages, Members can maintain their exception records without having to know the current status of the record on the VEAS files. For instance, VEAS accepts attempts to add a record for a Cardholder that is already in the file as a change request. For more information about the Exception File and the Cardholder Database, see *System Management for Members*.

#### A.7.1.1 Member Processor computer interface

The interface sends updates directly to the VIC or indirectly through a Visa Europe System connection. VEAS performs file maintenance in real time, and it updates the file as soon as it receives the message; the effective update time is the date and time that the update occurs.

Member Processors may send updates at any time while they are signed on to the network. Members do not use passwords, but the VIC does verify that the Member Processor is authorized for file access. Visa Europe can ask Member Processors not to update their files during peak volume hours when system response time is slow due to heavy authorization traffic. For details about updating, refer to the description of file update message types 0120 and 0322 in Chapter 4, *DMSA messages and flows*.

#### A.7.1.2 Individual updates through Visa Europe System connections

Member Processors equipped with a Visa Extended Access Server (EA Server) can send individual updates to the VIC. As with updates from a computer interface, VEAS applies terminal updates to the file in real time, and the effective date is the date that the VIC receives the updates.

For online file update messages, the file name (field 101) in the message indicates the file that is being updated. When updating address and PIN Verification data online, Issuer Processors use File Name A2 to process address verification data and File Name P2 to process PIN Verification data.

### A.7.1.3 File maintenance errors

A file maintenance message that contains errors does not update the file. When VEAS returns response code 06 in a file maintenance response, the response code indicates that the request contains an error. The response message also contains a 4-digit code in field 48 - Additional Data - Private that identifies the error. For valid reject codes, refer to *the DMSA Technical Specifications*.

All messages must meet the requirements described in the *DMSA Technical Specifications*.

## A.7.2 Batch update process summary

Issuer Processors can use batch processing to update Cardholder records in the Cardholder Database. The process consists of creating offline batch files and sending them to the VIC by courier (or other secure method).

DMSA and SMS Issuers can perform a full file replacement for all Exception File records at the BIN level as well as at the PCR level. SMS Issuers can also update the Exception File with a tape file containing only one update per Account Number. For more information about full file replacement by batch processing, refer to the description of the *Cardholder Database in System Management for Members*, and the description of batch file maintenance in the *DMSA Technical Specifications*.

Table 45 shows the applicable parameters for the BIN-level full file replacement option.

**Table 45: Exception File full file replacement at BIN level**

| Exception File full file replacement at BIN level | | |
|---|---|---|
| **File characteristics** | **Processing rules** | |
| | **DMSA** | **SMS** |
| Media | DMSA Issuers may send a file replacement by transmitting a tape file1 to the VIC from an EA Server or by sending a tape to Visa Europe. | SMS Issuers may send a file replacement tape electronically to Visa Europe. |
| File Types | The Visa Europe System permits File types E1 and E2. | The Visa Europe System permits File types E1, E2, E3, and E4. |
| BIN Number in File Header Record | The file header record must contain the BIN number for the records to be updated in positions 41-51.<br>**Note** Issuers must right-justify the BIN number and zero-fill the field. | The file header record must contain the BIN number for the records to be updated in positions 41-51.<br>**Note** Issuers must right-justify the BIN number and zero-fill the field. |

| Exception File full file replacement at BIN level | | |
|---|---|---|
| **File characteristics** | **Processing rules** | |
| | **DMSA** | **SMS** |
| Processing Type Code in File Header Record | The processing type code in position 14 in the file header record must be one of the following:<br>1 = Replacement of entire file by PCR<br>2 = Replacement of entire file by BIN<br>**Note** The use of processing type code U to update selected records remains unchanged. | The processing type code in position 14 in the file header record must be one of the following:<br>3 = Replacement of entire file by PCR<br>4 = Replacement of entire file by BIN<br>**Note** The use of processing type code U to update selected records remains unchanged. |
| File Update Code in Detail Record | The file update code in position 3 in the detail record must be 1 or 2. | The file update code in position 3 in the detail record must be 1, 2, 3, or 4. |

1. A tape file is a batch file of update or replacement records that are applied to the user files at the VIC. The batch file is usually written to a tape, but it may be a disk file that is transferred from a centre host to an EA Server.

### A.7.3 Member access to file records

Member Processors can request a record at any time while they are signed on to the network, although Visa Europe may restrict file access to low-volume hours, and the Member Processor must be authorized to access the specific file.

Except for the Activity File, Member Processors equipped with Visa Europe System connections can use online messages to review a Cardholder's record. The system displays all Member Processor-maintained fields; however, it does not display all of the fields added by or maintained by the Visa Europe System. The Member Processor can also request reports of Advice File and Exception File records.

For details about online file inquiry requests, see the description of message types 0120 and 0322 in Chapter 4, *DMSA messages and flows*, and in the *DMSA Technical Specifications*.

## A.8 Advice file

### A.8.1 File description

Each VIC maintains an Advice File containing records of STIP responses. Each record includes information from the authorization or reversal request, the STIP response, and the reason why STIP processed the request.

### A.8.2 File content

The advice file can contain:

- 0120 authorization advices, including those for Account Number or address verifications
- 0420 reversal advices
- 0120 and 0322 advices of Exception File additions and changes processed by the Visa Europe System for the following services:
  - Chargeback Reduction Service (T&E Chargeback processing)
  - Auto-CDB Service
- 0120 and 0322 discrepancy advices of Exception File update requests that the Visa Europe System could not process for the Issuer Processor when submitted using an enhanced Authorization Response
- 0120 and 0322 Account Number verification request advices of file updates

For a description of the DMSA Advice Retrieval Service, refer to *Visa Europe Authorization Services*.

### A.8.3 Unique fields

Advices contain specific fields from the original request and response messages. For details about the fields contained in advice messages refer to the *DMSA Technical Specifications*.

### A.8.4 Maintenance and update

VEAS keeps advice records on file at the VIC for 15 days. Issuers can recover their advice records by using online messages or by receiving advice records through DMSC.

### A.8.5 Purging records

VEAS purges records in the Advice File after Issuers recover them or when Issuers do not recover them within 15 days.

# B Summary of DMSA processing services and capabilities

DMSA processing support includes the following capabilities, services, and Visa Card Product family enhancements:

- Account Funding Transaction processing rules
- Account-level programs and Cardholder rewards
- Account Verification or address verification - only status checks
- Card Verification Service (CVV, iCVV, and CVV2)
- Contactless processing (dCVV)
- Authorization Gateway Services
- Custom Payment Service
- Incremental authorization processing
- Instalment payment service
- MasterCard processing through the Visa Europe System
- Merchant Verification Value processing
- Partial Authorizations
- Prepaid activation, load, and Partial Authorization processing
- Priority Routing Service
- Real Time Scoring Service
- Recurring payment processing
- Verified by Visa Service and Electronic Commerce Transactions (CAVV)
- Visa cash back processing - Visa cash back Service
- Visa Commercial Card large ticket transactions
- Visa Europe Payment Token Service
- Visa product eligibility inquiries
- Visa Smart Debit/Credit

## B.1 Account Funding Transaction processing rules

An Account Funding Transaction (AFT) can be used by Acquirers and originators to debit funds from a sender's account. Acquirers and originators can then use money transfer Original Credit transactions (OCTs) to push the funds to a recipient's account. It is recommended that when a Visa Card is used to fund an OCT, an AFT be used to debit funds from the sender's Visa account.

Acquirers and originators may optionally include the usages of fields 28 and 54 for AFT fee amounts in AFT DMSA and SMS request messages. If included in DMSA request messages, the fees must be also be included in subsequent DMSC transactions.

Issuers may choose to receive either the usage of field 28, the new amount type for field 54, or both, in AFT DMSA and SMS request messages.

Issuers can use these fields to comply with local regulatory requirements, or to include the fees on Cardholder's statements, or for Cardholder inquiries.

When an AFT 0100 Authorization Request or a 0200 full financial request message is received:

- If both of the following conditions are true, DMSA and SMS rejects the request message with a value of 0150 (Invalid value):
  - Field 54 is present
  - The value in the Amount subfield is not correctly formatted
- If both of the following conditions are true, DMSA and SMS declines the request message with a value of 12 (Invalid transaction):
  - Field 54 is present
  - The Currency Code subfield is not the same value as in field 49

### B.1.1 Enhanced money transfer OCTs

The processing rules are as follows.

If all of the following conditions are true VEAS declines the transaction with the response code 64 (transaction does not fulfil AML requirement):

- An enhanced money transfer OCT 0200 Full financial message is received
- The Source of Funds tag in field 104, dataset 5F is not present
- The recipient Issuer is in the US region

If all of the following conditions are true VEAS removes the Source of Funds tag from the request message before forwarding to the recipient Issuer:

- An enhanced money transfer OCT 0200 Full financial message is received
- The Source of Funds tag in field 104, dataset 5F is present
- The recipient Issuer is not in the US region

All Acquirers and originators are able to initiate enhanced money transfer OCTs for US-issued Credit Card accounts.

### B.1.2 Online gambling block for OCTs

Online gambling OCTs are identified by field 18 - Merchant Type, with a value of 7995 (Betting, including Lottery Tickets), and field 25 - Point-of-Service Condition Code, with a value of 59 (Electronic commerce request by public network). There are processing rules in DMSA, SMS, and DMSC to block domestic online gambling OCTs destined to recipient Issuers in Bangladesh, Nepal, and Vietnam.

DMSA or SMS declines the transaction with the response code value of 93 (transaction cannot be completed - violation of law) when a 0100 Authorization Request or a 0200 full financial request is received where all of the following conditions are true:

- The recipient Issuer is in Bangladesh, Nepal, or Vietnam
- Field 3 - Processing Code, positions 1-2, Transaction Type = 26 (Original Credit)
- Field 18 = 7995
- Field 25 = 59

## B.2 Account-level programs and Cardholder rewards

The Visa Incentive Network (VIN) allows Visa Canada and US region Members and Merchants to design and implement unique products and services for individual Cardholders or for highly specific groups of Cardholders. Visa has unlinked the services and benefits that were associated with the Visa Classic, Visa Gold, and Visa Platinum programs. The three Cards are combined as the Visa Consumer Credit Platform, and Issuers can define the benefits that distinguish their Classic, Gold, and Platinum consumer credit products as they see fit.

By establishing standards for a Visa Consumer Credit Platform rather than defining distinctions among Classic, Gold, and Platinum, Issuers can define the benefits that distinguish the Cards. Issuer-defined products (for instance, Classic, Gold, Platinum) may reside in the same BIN. Also, all Visa Consumer Credit Platform Cards carry auto rental insurance as a basic feature paid entirely by Visa.

With the Consumer Credit Platform, Issuers can track consumer Card-level activity by individual Account Number. This ability enables participating Issuers to assign multiple features and modify products, services, and enhancements without changing the Account Number or reissuing the Card. The Card-level capability applies to Visa traditional products (consumer Credit Card types without reward programs) and Visa traditional rewards products (consumer credit programs with reward programs) processed as DMSA 01xx dual-message or SMS 02xx full financial consumer Card-based transactions, including their reversals.

Account-level processing is available also for certain commercial and prepaid products.

For account-level processing, in addition to the Account Number, a key field in a Card-level program is field 62.23 - Card-Level Results. VEAS adds this field to authorization or financial requests to identify the specific Card project for the Issuer. VEAS retrieves the values from the CDB according to the specific Cardholder. Issuers update the CDB with the Cardholder Maintenance File. Refer to the technical specifications listed in Section 1.6, *Related information*, for more information.

## B.3 Account Verification or address verification - only status checks

See Section 6.10, *Account Verification or address verification-only status checks*, for further information.

## B.4 Card Verification Service (CVV, iCVV, and CVV2)

Issuers can verify the following values themselves, or choose to have VEAS verify the values on their behalf, either all of the time or only when the Issuer is unavailable and STIP processes the transaction.

- A CVV is a 3-digit number encoded on the Card's physical magnetic stripe or in the Chip's image on a VSDC Card
- An iCVV is a 3-digit number that Issuers may encode in the Chip's image on a VSDC Chip Card instead of the CVV

  The iCVV is also referred to as the alternate CVV. The Chip image on a VSDC Card may contain either the CVV or the iCVV. An iCVV is not used on a Card's physical magnetic stripe.

- The CVV2 is an embossed 3-digit security number appearing on the reverse side of the Card

  This can be used in both Card-present and Card-not-present transactions.

Visa Europe offers a verification service for the following:

- CVV or iCVV for Card-present transactions
- CVV2 for Card-present and Card-not-present transactions

**Note** Visa allows CVV and CVV2 emergency replacements for Visa Electron Cards for all regions except the US and Canada.

### B.4.1 CVV and iCVV

Determining whether VEAS is to verify the CVV or the iCVV depends on the Issuer's system parameters and on the code in field 22 - Point-of-Service Entry Mode Code in the request. Also, VEAS performs CVV processing only if the CVV is in the correct position in the track. For technical specifications for CVV placement, refer to the *Payment Technology Standards Manual*.

Whether to verify the CVV or the iCVV is determined as follows:

- If field 22, positions 1 and 2, contain 90 or 05 and the Issuer's system settings indicate that VEAS is to perform CVV checking, the security module performs the verification using the CVV algorithm

  Validation of the CVV from the physical magnetic stripe does not occur if field 22, positions 1 and 2, contain 02 or 95, because the values 02 and 95 indicate that the track data in field 35 - Track 2 Data or in field 45 - Track 1 Data may be unreliable and accurate CVV processing may not be possible.

  **Note** For Plus ATM transactions only, the value 02 indicates that the exact contents of Track 2 were read and that CVV checking is possible. For Visa ATM Transactions, values 02 or 90 can be used to indicate that the complete, unaltered magnetic stripe content has been read and that CVV processing may not be possible.
- If field 22, positions 1 and 2, contain 05, VEAS assumes that the track data originated from the Chip

  VEAS checks the Issuer's system settings in the Customer Online Repository (CORE) to determine whether the Issuer is encoding the iCVV on the Magnetic Stripe Image and, if so, determines the earliest expiry date that a Card could have if it has an iCVV:

  - If the Issuer's system settings indicate that it supports CVV checking for Chip Cards but does not support iCVV checking, the security module performs the verification using the CVV algorithm
  - If the Issuer's system parameters indicate that it supports both CVV checking and iCVV checking for Chip Cards, the security module performs the verification using the CVV algorithm except that the system substitutes 999 for the service restriction code

  **Note** The presence of POS Entry Mode 90 in field 22 does not guarantee CVV processing. If a non-participating Acquirer submits POS Entry Mode 90 in field 22, VEAS rejects the message.

Validation of the CVV or the iCVV residing in the Magnetic Stripe Image of the Chip does not occur if field 22, positions 1 and 2, contain 95, because the value 95 indicates that the track data in field 35 or in field 45 may be unreliable.

To verify the CVV, VEAS (or the Issuer) uses the Triple Data Encryption Standard (TDES) key and other information from the stripe to calculate a CVV and then compares it with the stripe's encoded CVV. For the CVV to be valid the two values must match exactly; otherwise, the CVV fails validation.

The iCVV processing uses all options, parameters, and keys used in CVV processing. VEAS or the Issuer uses the same algorithm both for the CVV and for the iCVV, but they substitute the value 999 for the service restriction code for iCVV processing. As part of the Issuer participation procedure, the Issuer specifies appropriate expiry date ranges and whether the CVV check is to be based on the Chip image of the magnetic stripe data.

STIP can respond to CVV failures with an Issuer-specified Decline Response code or can forward failures to the Issuer for processing. Issuers or VEAS can approve, refer, or decline transactions that fail CVV validation depending on Issuer-specified parameters.

For a description of CVV validation, refer to the *Visa Europe Technical Service Descriptions*. For technical specifications for CVV placement, calculation and verification, refer to the *Payment Technology Standards Manual*.

### B.4.2 CVV2

Members use CVV2 processing for Card-not-present transactions and for Card-present transactions. The presence of field 126.10 - CVV2 Authorization Request Data in an Authorization Request indicates the presence of the CVV2 value.

**Note** In transactions made with all Card types, a value of 1 in field 126.10, position 1, indicates that the transaction contains the CVV2 or CVV2 equivalent, and a value of 1 in field 126.10, position 2, indicates that the Acquirer wants the Issuer to return the CVV2 results value in field 44.10.

If the Issuer participates in the CVV2 Service, the VSM uses the CVV2 algorithm to validate the CVV2 value (a 3-digit security number), which Issuers emboss on the reverse side of the Card. The algorithm uses the Card's embossed Account Number and its expiry date to recalculate a CVV2, which VEAS compares with the CVV2 value read from the reverse side of the Card. A match increases the probability that the Cardholder is authentic. Authorization Responses contain the CVV2 result values in field 44.10 - CVV2 Result Code. Response Code N7 - Decline for CVV2 Failure in field 39 - Response Code indicates failed matches.

Issuers can perform their own CVV2 validation, or can have VEAS validate the CVV2 for them, or can do both. If VEAS performs the validation, it verifies the CVV2 before it passes the Authorization Request to the Issuer or to STIP. Issuers can choose to have VEAS check the CVV2 in all CVV2-eligible Authorization Requests.

**Note** If a request contains both a CAVV and a CVV2, CAVV validation takes precedence over CVV2 validation. For further information concerning VEAS processing when both elements are present in a request, refer to the *Visa Europe Technical Service Descriptions*.

Depending on regional requirements and on Issuer participation, VEAS can restrict Card-present CVV2 processing by bypassing CVV2 Service processing entirely and directly passing field 126.10 to the Issuer. This **pass-through** case is separate from the CVV2 Service; VEAS does not populate field 44.10 or field 39 in 0100 requests or in 0110 responses based on field 126.10 data. Issuers that want to receive CVV2 data in Card-present **pass-through** transactions can also participate in the CVV2 Service.

VEAS supports CVV2 verification-only requests. For such requests, field 25 - Point-of-Service Condition Code must contain 51, field 3 - Processing Code, positions 1-2, must contain 39 (eligibility message), 70 (PIN change/unblock), or 72 (PIN unblock or prepaid activation), and field 126.10 - CVV2 Authorization Request Data must be present. If the request meets all the verification-only field requirements, and field 4 contains an amount other than zero, STIP ignores the amount and, if the request is successful, responds with a value of 85 (no reason to decline) in field 39.

For a description of CVV2 verification, refer to the *Visa Europe Technical Service Descriptions*.

## B.5 Contactless processing (dCVV)

Cardholders make contactless transactions using contactless Chip Cards and mobile devices. A dCVV resides in the contactless Card. dCVV verification processing occurs when a terminal or contactless device equipped to accept contactless Chip Cards reads the Chip Card. The contactless Chip creates the dCVV value and inserts it into the Track 1 or Track 2 magnetic stripe data that it transmits to the terminal along with other data. The dCVV replaces any CVV data that may have been in the track data.

Visa contactless Cards are one of the following:

- A magnetic stripe Visa Card with an embedded contactless Chip
- A VSDC Chip Card that has a magnetic stripe and supports a contactless Chip

  **Note** Members that want to accept and process VSDC Chip Cards for contactless transactions must be participants in the VSDC Service.

A Card can include a contactless Chip with its dCVV algorithm as well as a CVV in the Track 1 or Track 2 magnetic stripe. A VSDC Chip Card can also contain a contactless Chip with its dCVV algorithm as well as a CVV or an iCVV.

VEAS identifies a contactless authorization or financial request if the POS Entry Mode code in field 22 is 07 (contactless Chip Transaction originated using VSDC Chip data rules) or is 91 (contactless Chip using magnetic stripe data rules).

Additionally, in the Visa US region, Acquirers must insert code 8 in field 60.2 - Terminal Entry Capability. Acquirers in other regions do not have to use code 8 in field 60.2.

## B.6 Authorization Gateway Services

See Section 7.5.5, *Gateway Services*, for further information.

## B.7 Custom Payment Service

The Custom Payment Service (CPS) protects Merchants and Acquirers against authorization-related Chargebacks by requiring the Authorization Request to contain certain key

information that might not otherwise be present. VEAS matches a transaction's clearing and authorization messages using a unique Transaction Identifier (TID) assigned by VEAS before it forwards requests to Issuers or to STIP. CPS processing applies to Visa Card POS transactions, to International Transactions and Plus ATM transactions, and to Visa Secure Electronic Commerce (VSEC) transactions.

Merchants in specific market segments qualify for various CPS fees by meeting associated fee edit criteria. There are specific fee edit criteria for each CPS program.

CPS requires Acquirers to include field 62.1 - Authorization Characteristics Indicator to signal to DMSA that the transaction is being submitted for CPS qualification. Acquirers include other key field information in Authorization Requests as well. Issuers can accurately match a transaction's clearing and authorization messages using a unique TID in field 62.2 - Transaction Identifier. VEAS assigns a TID in field 62.2 to all transactions before DMSA forwards the request to the Issuer or to STIP. See Appendix B.11, *Merchant Verification Value processing*.

VEAS uses the values in field 60.1 - Terminal Type and field 60.2 - Terminal Entry Capability to determine specific transaction types.

**Note** DMSA only accepts CPS transactions in bitmap format. Bitmap format is required for participation in the full range of CPS markets; the older fixed format is not valid in Visa Europe.

For CPS/ATM information, refer to the description of Custom Payment Service/ATM in the *Visa Europe Technical Service Descriptions*.

## B.8 Incremental authorization processing

Certain Merchants, such as Hotels, Car Rental Companies, and Airlines, initiate incremental authorization transactions when the final amount of the purchase is unknown. The incremental authorization contains an estimated amount that may vary significantly from the final Transaction Amount. When the Merchant determines the final amount, it submits a supplemental, or incremental, authorization or a single authorization reversal if the purchase is cancelled.

## B.9 Instalment payment service

Allows the Acquirer to accurately identify the Instalment Transaction, and the Issuer may use the indicator to identify the type of payment transaction that is being approved.

Acquirers may choose to submit Instalment Transaction messages with optional instalment payment data in field 104 in TLV format.

Acquirers that submit instalment payment data in field 104 must be prepared to receive it in response messages.

An Acquirer submits an instalment payment authorization, and the Issuer is not certified to receive field 104. VEAS drops field 104 prior to sending the message to the Issuer.

**Note** If instalment payment data is submitted in the authorization, it must also be submitted in the Clearing Record.

## B.10 MasterCard processing through the Visa Europe System

**Credit POS processing** - Gateway Services route non-PIN POS MasterCard transactions from Visa Acquirers to MasterCard issuers, automatically converting the Visa Europe System-format messages to MasterCard's Banknet format. Similarly, Gateway Services automatically convert Banknet-format responses from issuers to the Visa Europe System format for delivery to Visa Acquirers.

**ATM processing** - DMSA does not send PIN-based MasterCard transactions to Banknet; VEAS declines them with response code 91 (cryptographic error found) in field 39. The Visa Europe System supports PIN-based Cash Disbursement transactions if the Issuer can receive them directly through the Visa Europe System as 0200 full financial messages destined for Plus or CIRRUS SMS Issuer BINs.

MasterCard transactions or transaction elements supported by Visa Europe include the elements in Table 46:

**Table 46: MasterCard transactions or transaction elements supported by Visa Europe**

| MasterCard transactions or transaction elements supported by Visa Europe | |
|---|---|
| Account Verification | Merchant Advice Code |
| Address Verification | Partial Approvals |
| Balance Inquiries | Partial Approval Reversals |
| Chip-Based Transactions | Proximity/Contactless Payments |
| Requests with CVC1 and CVC2 | Recurring Payments |
| Electronic Commerce | Recurring Payment Cancellations |
| MasterCard Corporate Fleet Card Program | Transponder-Based Transactions |
| MasterCard Travel Industries Program | Telephone Orders With UCAF Data |

The *Authorization Gateway Service Cross-Reference Guide* describes these transactions and elements. The gateway also sends Visa Europe System-acquired Diners Club Authorization Requests with Diners Club or MasterCard Account Numbers to the Discover network; the Visa Europe System no longer routes Diners Club requests to Diners Club.

For details about how the gateway function transfers data between networks, refer to the *Authorization Gateway Service Cross-Reference Guide*. This document includes field-by-field data transfer descriptions between Visa Europe System-format dual-message 0100 Authorization Requests and Authorization Responses, and American Express- and MasterCard-format Authorization Requests and responses. It also contains key field summaries for different American Express and MasterCard services and functions supported by the Visa Gateway.

### B.10.1 MasterCard Gateway multicurrency processing

If Visa Acquirers of MasterCard transactions participate in the Visa Multicurrency Service, the request and response messages remain by default in the Acquirer's local currency - the Visa Europe System does not convert amounts to US dollars (USD). For requests, the Visa Gateway transfers the Visa Europe System field 4 amount to Banknet DE 4 while retaining the

Acquirer's local currency, and it transfers the currency code from Visa Europe System field 49 to Banknet DE 49 without changing the Acquirer's original code.

VEAS does not include field 6 - Cardholder Billing Amount, field 10 - Cardholder Billing Conversion Rate, and field 51 - Cardholder Billing Currency Code in the messages.

In responses, the process is reversed; the response message to the Acquirer indicates the Acquirer's original currency. The Visa Gateway discards any other multicurrency field that Banknet may include in the MasterCard response.

Visa Acquirers of MasterCard transactions that do not participate in the Visa Multicurrency Service continue to have their messages' field 4 and DE 4 amounts converted to USD and VEAS changes the currency code in field 49 and DE 49 to 840. Additionally, VEAS also changes the currencies in 0100 MasterCard Authorization Requests sent by Visa SMS Acquirers to Banknet to USD, regardless of the currency type originally assigned.

The only editing VEAS performs is to ensure the field 49 currency code in the request message is valid. VEAS rejects the message if the currency code is invalid.

Participation in this MasterCard multicurrency feature is optional, but both the Processing Centre and acquiring BIN must participate.

## B.11 Merchant Verification Value processing

VEAS uses the Merchant Verification Value (MVV) to identify Merchants. The MVV is unique to the Merchant and Merchants include it in field 62.20 - Merchant Verification Value in authorization and reversal requests. Visa Europe assigns the first six positions and helps the Acquirer assign the last four; if the field format is invalid in requests, VEAS drops the field. Acquirers and Issuers must be certified to receive this field. The MVV is not necessarily a component of the Custom Payment Service.

## B.12 Partial Authorizations

The Visa Europe System supports Partial Authorizations involving multicurrency processing for Prepaid Cards processed as DMSA dual-message and SMS single-message transactions for all regions. Responses can include account balances along with the Partial Authorization amounts. (Standalone balance inquiries operate under different requirements.) Acquirers must include code 1 in field 60.10 - Partial Authorization Indicator to indicate that the terminal supports Partial Authorizations.

**Note** This field is optional for Acquirers. Only Acquirers that participate in the service may submit this field. This field is sent only to participating Issuers.

### B.12.1 Key fields and rules for Partial Authorizations with multicurrency processing

Table 47 lists Partial Authorization key fields for 0110 and 0210 responses.

**Table 47: Key fields for Partial Authorization 0110 and 0210 responses**

| Key fields for Partial Authorization 0110 and 0210 responses | |
|---|---|
| **Field** | **Description** |
| Field 4 - Transaction Amount | Contains the Partially Authorized amount from the Issuer. |
| Field 6 - Cardholder Billing Amount | Contains the amount in field 4 in the Billing Currency of the Cardholder if multicurrency processing is involved in the transaction. |
| Field 39 - Response Code | Contains response code 10 for Partial Authorizations. |
| Field 54 - Additional Amounts | This field contains the amount in field 4 from the original 0100 authorization or 0200 financial request. Field 54 has the capacity for six **sets** of amount data; for instance, the original amount in field 4 followed by an account balance.<br>Each set comprises position 1 through position 20; set two begins with position 21, and so on. Multicurrency processing involves more than one set. Issuers must populate this field beginning with the first available set; that is, position 1, position 21, and so on. The field positions for partial approvals are:<br>Positions 1-2 - Account Type: These positions contain a 2-digit code that identifies the account providing the amount, for instance, 10 (savings account) or 20 (checking account).<br>Positions 3-4 - Amount Type: These positions contain code 57 (for original amount).<br>Positions 5-7 - Currency Code: These positions contain a 3-digit code that identifies the amount in positions 9-20.<br>Position 8 - Amount Sign: This positions contains code C (positive balance) or D (negative balance)<br>Positions 9-20 - Amount: These positions contain a 12-character amount. |

**Note** Issuers must return field 51 in partial approvals when field 6 is present.

**Note** If the converted Transaction Currency amount in field 54 exceeds the 12-character converted amount limit, the converted currency amount value is 999999999999 (12 nines).

VEAS returns the Issuer's response with reject code 0150 if field 39 contains response code 10, but field 54 contains any of the following errors:

- The field is missing

- The Partial Authorization data set does not begin in the first available position
- An empty set exists between two populated sets

If field 54 is present and correctly formatted, but field 39 does not contain response code 10, VEAS returns the transaction to the Issuer with response code 0486. If the Issuer supports multicurrency processing, but the amount in field 6 in the response is greater than the amount in field 6 in the request, VEAS returns the transaction to the Issuer with response code 0736.

If the original Transaction Amount is not present in field 54 for a Partial Authorization, VEAS inserts the original amount in field 54 before forwarding the 0110 response to the Acquirer.

If a transaction is rejected back to the Issuer, VEAS will invoke STIP, which accepts or declines the total Transaction Amount using Issuer-specified parameters.

Because the order of the field 54 amount sets cannot be guaranteed, Acquirers should check the account type, the amount type, and the currency code subfields to determine what the set represents.

### B.12.2 Partial Authorizations with no multicurrency processing rules

If the 0110 or 0210 response contains response code 10 in field 39, and field 4 is missing, VEAS returns the transaction with reject code 0275 (field missing). If the amount in field 4 of the response is greater than the amount in field 4 in the request, VEAS returns the transaction with reject code 0735 (Partial Authorization field 4 value is greater than the original field 4 Transaction Amount). In either case, STIP approves or declines the transaction using Issuer-specified parameters. If the original Transaction Amount is not present in field 54 in a Partial Authorization transaction, VEAS inserts the original amount in field 54 before forwarding the response to the Acquirer.

**Note** VEAS drops field 54 from the response before forwarding it to the Acquirer if the Acquirer does not participate in POS balance services.

For reversals of Partially Authorized transactions, field 95 - Replacement Amounts contains the partially approved amount from field 4 in the 0110 or 0210 response (not the original amount in field 4 in the 0100 or 0200 request).

The processing rules to support additional amounts for AFD transactions are as follows.

An 0100 Authorization Request is submitted with the following:

- Field 4 - Amount, Transaction = n (Valid transaction amount up to the maximum Visa Europe amount of EUR 150.00 or local currency, unless a higher amount is pre-selected by the Cardholder at the pump)
- Field 18 - Merchant Type = 5542 (Fuel Dispenser, Automated)
- Field 60.10 - Partial Authorization Indicator = 1 (Terminal accepts Partial Authorization responses)

If the Issuer participates in processing Partial Authorizations, it can include an additional approved amount in the 0110 Authorization Response.

If an additional approved amount is received by Visa Europe, the following information is present in the 0110 Authorization Response to the Acquirer:

- Additional approved amount from the Issuer is placed in field 4

- A response code of 10 (Partial Authorization) is present in field 39 - Response Code
- The original amount is included in field 54 - Additional Amounts with an amount type of 57 (Original amount)

If the Issuer does not participate in Partial Authorizations, existing response codes are sent in the 0110 Authorization Response.

### B.12.3 Processing balances with multicurrency processing and optional Issuer fees

For field 54 sets that contain balance information in cross-border transactions, if the Billing Currency of the Cardholder is not the same as the Transaction Currency, VEAS replaces the balance amount in the Billing Currency with the balance amount converted to the Transaction Currency, minus the optional Issuer currency conversion fee.

The Optional Issuer Fee (OIF) rates for Partial Authorization transactions using Prepaid Cards involving multicurrency processing may vary between the time a transaction is authorized and the time it is settled. For Prepaid Cards, if the OIF rates between authorization and settlement differ, the Settlement Amount of the transaction may not be the same as the authorized amount.

For Issuers performing their own multicurrency processing, if the Billing Currency is not the same as the Transaction Currency in cross-border transactions, multicurrency participating Issuers should first deduct the OIF from the balance amount on Prepaid Cards before sending the balance to the Acquirer. VEAS does not deduct the OIF from the balance amount when it converts the balance from the Billing Currency to the Transaction Currency.

## B.13 Prepaid activation, load, and Partial Authorization processing

VEAS processes Prepaid Cards for Visa and private-label Card products. Merchants and Issuers submit transactions to activate new Prepaid Cards and to load spending amounts onto activated Cards.

Merchants and Issuers can submit load requests without submitting activation requests, and can activate and load value to Cards in a single request message.

Merchants and Issuers submit activation or load void requests, or reversals, for Cards that are activated or loaded in error. Merchants and Issuers can submit a void only on the same day as the original request.

**Note** An emergency shutoff flag in VEAS shields POS load Issuers from receiving ATM loads.

When Merchants submit authorizations for an amount that is greater than the amount loaded onto the Card, Issuers can return Partial Authorizations for the available amount on the Card; see Appendix B.12, *Partial Authorizations,* for more information.

Prepaid transactions, including Partial Authorizations, are eligible for STIP.

Participation in Prepaid Card processing services is optional for Issuers, Acquirers, Processors, and Merchants. Acquirers that want to participate are required to support partial approval amounts. Issuers that want to participate are required to support the Partial Authorization value in request messages, but may optionally support Partial Authorization responses. Both Acquirers and Issuers must be certified that they can send and receive prepaid transactions.

## B.14 Priority Routing Service

The Priority Routing Service enables SMS Acquirers to accept transactions that are destined for either the Visa or Plus networks and enables Visa Europe Authorization Service (VEAS) to determine the preferred network and the set of programme rules to use for each transaction. Acquirers can request priority routing only for authorizations, status-check authorizations, Original Credits, original financial transactions and reversals.

Acquirers do not need to assign a specific network identification code in the Authorization Request; VEAS automatically selects the most appropriate network and routes the request accordingly.

## B.15 Real Time Scoring Service

The Visa Europe Real Time Scoring Service (RTS) enables Issuers to receive information on the likelihood of a transaction being fraudulent in the time it takes to process an Authorization Request.

RTS can instantly create a case and incorporate the risk score into the Authorization Request, enabling Issuers to factor this information into their authorization decisions and to detect fraud faster and more accurately.

The risk score is based on the Cardholder's previous spending patterns and transaction history. It also takes account of the individual fraud experience of the Merchant. Cardholder profiles are continuously updated as transactions are processed and Merchant profile data is also regularly updated.

## B.16 Recurring payment processing

A recurring payment transaction is one that occurs on a periodic basis per an agreement between the Cardholder and the Merchant for payments for goods and services such as utility bills and magazine or online subscriptions. The initial transaction can occur in a Card-Present Environment (such as face-to-face POS) or a Card-Absent Environment, such as mail order/telephone order (MOTO) or e-commerce. Merchants automatically initiate subsequent, or recurring, transactions without the Cardholder being notified beforehand or necessarily being present.

The presence of 02 of R in field 126.13 - POS Environment identifies the transaction as a recurring payment Authorization Request.

A value of 02 in field 60.8, positions 9-10, is mandatory for recurring payment transactions acquired in the US region and is optional for non-US-acquired transactions. A value of R in field 126.13 is required for recurring payment transactions originating from an Acquirer outside of the US region and is optional for US-acquired transactions. Depending on the region, Acquirers may send both fields with their recurring payment codes in the same request.

Both fields and their values are valid for Chargeback protection. If the Issuer is not certified to receive field 126.13, VEAS drops it before forwarding the request to the Issuer and inserts code 02 in field 60.8.

The Visa Europe System force-routes recurring payment requests to Issuers. For Issuer-unavailable conditions, STIP processes the request according to Issuer-specified parameters as if recurring payment specifications were not involved.

STIP declines recurring payment transactions made with Cards whose expiry dates have expired or are missing. Issuers can choose, however, to have STIP approve these transactions according to Issuer-specified parameters.

## B.17 Verified by Visa Service and Electronic Commerce Transactions (CAVV)

The Verified by Visa Service (VbV) is a risk control service used to authenticate the Cardholder in electronic commerce (e-commerce) authorization transactions. VbV utilises the Cardholder Authentication Verification Value (CAVV) Service. The process involves two phases:

1. Verified by Visa
2. CAVV Verification

During the Verified by Visa phase, the Cardholder is electronically identified and a CAVV is generated that is associated with the purchase authorization.

The CAVV Service processing begins when the Acquirer submits the authorization or the full financial message and includes the CAVV (in field 126.9 - CAVV Data) that was generated during the Verified by Visa phase in the request. When the CAVV is present in the transaction, the Issuer or VEAS verifies that the CAVV in the message matches the CAVV generated during the Verified by Visa phase. If VEAS or the Issuer verifies the CAVV, the transaction is protected from certain Chargebacks should disputes arise later.

When the Issuer or VEAS (depending on who performed the validation), completes the validation process, it places the results in field 44.13 - Card Authentication Verification Value (CAVV) Result Code. The value in this field indicates the outcome of the validation, where the validation was performed, and the classification of the transaction: Authentication, Attempt, or Non-Secure.

To validate the CAVV, the Issuer or VEAS on behalf of the Issuer, uses Triple Data Encryption Standard (TDES) keys and other CAVV parameters to calculate the CAVV and then compare it to the CAVV generated by the appropriate Access Control Server (ACS). Issuers that choose to have VEAS perform verification on their behalf must provide Visa Europe with their TDES keys.

**Important** Visa has adopted the industry-standard Triple Data Encryption Standard (TDES). This change applies to all Members and covers all PIN-based Visa credit and debit, and Plus transactions processed through the Visa Europe System. All Visa Europe System endpoints must use TDES Issuer Working Keys (IWKs) and Acquirer Working Keys (AWKs).

Visa Europe offers two classifications of CAVV verification processing options to Issuers that participate in Verified by Visa: Authentication or Attempt. Visa Europe encourages Issuers to participate in both options.

- **Authentication**

  With this option, the Issuer is a full participant in the service and has Cardholders enrolled in Verified by Visa. Visa Europe classifies a transaction as an Authentication when the Acquirer, the Issuer, and the Cardholder all participate in Verified by Visa.

- **Attempt**

  With this option, the Issuer or VEAS generates a CAVV for attempted transactions. Visa Europe classifies a transaction submitted by a participating Acquirer as an Attempt when either the Issuer or the Cardholder does not participate in Verified by Visa. Liability shifts for these types of transactions. Visa Europe highly recommends that Issuers use this option.

Both options allow Issuers to select a predefined process by which their transactions should be processed by the Issuer and by STIP. The predefined processes are as follows:

- **VEAS does CAVV validation and declines failures**

  VEAS performs all validations on the Issuer's behalf, declines transactions when the CAVV validation fails, and forwards the status results of transactions that it does not decline to the Issuer

- **All CAVV results to Issuer**

  The Visa Europe System performs all validations on the Issuer's behalf, and forwards all status results of transactions to the Issuer

- **Issuer does its own CAVV validation**

  The Visa Europe System forwards the transactions to the Issuer to perform validation, and the Issuer returns the status results in the response messages

Depending on the region, the Visa Europe System assesses IRFs based on the CAVV Verification Service classification of the e-commerce transaction.

The CAVV Verification Service supports both magnetic stripe Visa Cards and VSDC Cards.

Certain transactions are ineligible for Verified by Visa and CAVV processing (the ECI in field 60.8 - Mail/Phone/Electronic Commerce and Payment Indicator or in field 63.6 is not 5 or 6) even though they may include a CAVV; for instance, the services do not support transactions involving Visa Business Cards, Visa Corporate Cards, or Visa Purchasing Cards. When VEAS validates a CAVV in an ineligible transaction, VEAS generates CAVV result code B in field 44.13. Only VEAS is allowed to generate this result code, which it uses for Visa-internal processing only.

Transaction aggregation allows Merchants to combine multiple e-commerce purchases made by the same Cardholder on the same Visa Europe account into a single, larger transaction and submit it for payment processing. Aggregation reduces Acquirers' IRFs. An e-commerce Merchant submits an Authorization Request for a specific or estimated total authorized amount. Merchants can submit multiple purchase requests up to three days or up to the authorized amount under the same Card without making additional Authorization Requests. Merchants submit a single clearing transaction at the end of three days or when the total authorized amount is met.

The market-specific authorization data Indicator (MSADI) transaction aggregation identifier (TAI) identifies an aggregation transaction for e-commerce basic and preferred programs. Field 62.4 - Market-Specific Data Identifier must contain the value E. If field 25 - POS Condition Code does not contain value 59 for e-commerce, VEAS changes the value in field 62.4 from E to N. VEAS makes this change before it calculates the validation code.

Acquirers with Merchants that choose to submit aggregated e-commerce transactions must support the new TAI in authorization and clearing transactions. E-commerce Merchants must support Partial Authorizations to allow Issuers to specify approval amounts below the estimated authorization amount. Issuers must be able to receive the new TAI in authorization and clearing transactions.

For more information about Verified by Visa, CAVV, and the CAVV verification key fields, refer to the *Visa Europe Technical Service Descriptions*, and to *the DMSA Technical Specifications*.

## B.18 Visa cash back processing - Visa cash back Service

The Visa cash back Service provides domestic cash back transaction capability for participating regions. Table 48 lists the cash back services supported by Visa Europe.

A domestic cash back transaction indicates that the Merchant, Acquirer, and the Issuer reside in the same country. Each Visa region can choose to implement cash back processing capability as a domestic-specific solution, or they can participate in the Visa cash back Service.

Cash back processing is optional for Issuers, for Acquirers, and for Merchants in all Visa regions. Participating regions and countries within those regions establish maximum cash back amounts. Regions that use the Visa cash back Service can control Member and country participation, and can set maximum cash back limits and different pricing options by country.

VEAS checks the Acquirer and the Issuer BINS, the Acquirer country code in field 19, and the Merchant country code in field 43 to determine if the POS cash back transaction is domestic. The cash back amount field is field 61.1 - Other Amounts. If the transaction is non-domestic, VEAS converts cash back amount in field 61.1 to the Issuer currency code and forwards the converted amount in field 61.2 to the Issuer.

**Table 48: Cash back services currently supported by Visa Europe**

| Cash back services currently supported by Visa Europe | | | |
|---|---|---|---|
| **Cash back services currently supported by Visa Europe** | **Availability** | **Cards** | **Card type** |
| Visa cash back Service | The Visa Europe Territory (excluding UK) | Visa, Visa Electron, VPAY | Debit and credit |
| UK cash back Service | United Kingdom only | Visa, Visa Electron | Debit only |

For further information about the Visa cash back Service, refer to the *Visa Europe Technical Service Descriptions*. Members interested in the service can contact Visa Europe Customer Support for details about participation.

## B.19 Visa Commercial Card large ticket transactions

Cardholders can use Visa Purchasing or Corporate travel and entertainment (T&E) Cards for Visa Commercial Card large ticket transactions. These government and non-government participant transactions involve amounts between USD 99,999.99 and USD 10,000,000.00. The program accommodates US General Services Administration (GSA), Intra-Government Transfer System (IGOTS), and intra-company Purchasing and Corporate T&E Transactions.

The maximum Transaction Amounts are as follows:

- USD 999,999.99 for Visa Signature Preferred and Visa Infinite
- USD 749,999.99 for Visa Signature and Visa Signature Business
- USD 9,999,999.99 for Visa Business, Visa Corporate, Visa Business Check Card, prepaid commercial, Visa Purchasing, Visa Purchasing with Fleet, Visa Purchasing GSA, Visa Purchasing GSA with Fleet, when the ARDEF participation flag (large ticket) is ON for the Card number
- Up to USD 749,999.99 for Visa Business, Visa Corporate, Visa Business Check Card, prepaid commercial, Visa Purchasing, Visa Purchasing with Fleet, Visa Purchasing GSA, Visa Purchasing GSA with Fleet, when the ARDEF participation flag (large ticket) is OFF for the Card number

STIP is not available for large ticket transactions between USD 500,000.00 and USD 10,000,000.00. STIP responds with response code 91 (Issuer unavailable) for Issuer-unavailable transactions or for transactions that have timed out. STIP processes Visa Commercial Card large ticket POS transactions under USD 100,000.00 using Issuer-specified processing rules.

VEAS declines the authorization messages with the response code of 13 (invalid amount) in field 39 - Response Code when an authorization message is submitted with the amount greater than USD 499,999.99 in field 4 and the product type is one of the following Visa Commercial Card products:

- Visa Business
- Visa Corporate
- Visa Purchase

See Section 5.5.6, *Editing Transaction Amounts*, for further information.

## B.20 Visa Europe Payment Token Service

The Visa Europe Payment Token Service is a payment token service that complies with the standards defined by the *EMV Payment Tokenisation Specification – Technical Framework*. A payment token is a surrogate for a Primary Account Number (PAN). The token replaces the PAN in transaction processing, thereby reducing the risk of a Cardholder's sensitive payment information being compromised.

**Important** Payment tokens issued by the Visa Europe Payment Token Service will be deployed to mobile devices and used for Visa payWave for mobile transactions and application-based e-commerce transactions. Other use cases may be enabled in the future.

The *EMV Payment Tokenisation Specification – Technical Framework* defines a number of new roles that are relevant to the payment token service offered by Visa Europe:

- Token Service Provider

  An entity that provides a payment token service. They provide payment tokens to registered Token Requestors, linking the payment token to the payment Card details provided in the request for a token. The Token Service Provider generates, issues and maintains tokens. They are also responsible for detokenising the token during transaction processing.

  The Visa Europe Payment Token Service fulfils the role of a Token Service Provider.

- Token Requestor

  A Token Requestor is an entity that has registered with a Token Service Provider to request payment tokens. Entities that may wish to register as a Token Requestor include Card Issuers, Card-on-file merchants, digital wallet providers, acquirers and payment service providers operating on behalf of merchants.

For more information see the *Visa Europe Payment Token Service: Product Overview*.

## B.21 Visa product eligibility inquiries

Visa product eligibility inquiries provide US consumer and commercial product information associated with the Cardholder's Account Number. VEAS does not forward these requests to Issuers. VEAS bases its responses on Card-level information or on account range details that VEAS retrieves from the system files. These US region-only 0100 Authorization Requests and 0110 responses are non-financial, information-only transactions. Product eligibility inquiries are valid for DMSA and SMS POS.

Account, address, or CVV2 verification-only requests can be used for status checks. The amount in field 4 can be zero in requests and their reversals, if:

- Field 3 - Processing Code, positions 1-2, contains 39 (eligibility message), 70 (PIN change/unblock), or 72 (PIN unblock or prepaid activation)
- Field 25 - Point-of-Service Condition Code contains 51 (zero amount Account Verification)
- Any of:
  - Field 52 - PIN Data and field 53 - Security-Related Control Information are present
  - Field 123 - Verification Data is present
  - Field 126.10 - CVV2 Authorization Request Data is present

Also, field 4 can be zero in 0302 file update requests or 9620 fraud advice requests. If the request meets all the verification-only field requirements, and field 4 contains an amount other than zero, STIP ignores the amount and, if the request is successful, responds with a value of 85 (no reason to decline) in field 39.

0110 responses include the key field 62.23 - Card-Level Results. VEAS populates this field with the Cardholder's consumer credit platform rewards program information from the Cardholder Database, the system files, or both. For consumer credit-only inquiries, the response also includes the field 62.23 value in position 6 of field 38 - Authorization

Identification Response. This field 38 condition does not apply to commercial and prepaid products in authorization and full financial responses.

US region Acquirers must be certified for the processing codes in field 3, field 22, and field 25, along with the ability to receive and process field 62.23. Participation is limited. Members can contact Visa Europe Customer Support for complete details.

## B.22 Visa Smart Debit/Credit

Visa Smart Debit/Credit (VSDC) is a Chip-based Visa Card Product that supports offline and online transactions, including Plus ATM transactions. VSDC Cards work in conjunction with special Chip-read terminals to approve or to decline transactions. VSDC offline transactions occur only between the Chip Card of the Cardholder and the terminal and do not go through the Visa Europe System. The Visa Europe System processes transactions online when processing triggers predetermined offline risk management procedures, or because of random selection parameters established by the Issuer.

For purchase transactions, the Issuer may determine whether a Cardholder signature or a PIN is required for Cardholder Verification. ATM Transactions require a PIN.

VSDC Cards rely on Cryptograms to ensure their security and the integrity of their offline and online transactions. Issuers that select the Full Data implementation option verify the Cryptogram submitted by Full Data Acquirers in the 0100 Authorization Request. The Card terminal authenticates the Cryptogram of the Issuer in the 0110 Authorization Response to ensure that the Issuer that created the Card is the Issuer that approved the transaction. If VEAS performs processing for the Card Authentication feature on behalf of the Issuer, VEAS validates the Authorization Request Cryptogram (ARQC) and provides the ARPC in the response. If the Issuer participates in the Issuer Authentication feature, either the Issuer or VEAS generates an ARPC that is sent to the Card in the response so the Card can validate that the Authorization Response came from the correct Issuer.

**Note** Issuer participation is optional in the VSDC Card Authentication feature and in the Issuer Authentication feature.

DMSA identifies a VSDC-based Authorization Request by the value in field 22 - Point-of-Service Entry Mode Code that indicates that a Chip Card was read at a VSDC terminal (05 or 95) and that the service restriction code in the magnetic stripe is 2 (international Card, alternate technology) or is 6 (national use, alternate technology).

VEAS processes VSDC transactions according to Card type. The Visa Europe System supports the following Card types:

- Visa Integrated Circuit Card Specification (VIS)

  This Card type uses the initial Chip Card type specifications for communicating between EMV (JCB, MasterCard, Visa) Cards and the Processors of their Issuers.
- Common Core Definition (CCD)

  CCD is a newer EMV Card type that contains the same data as a VIS Card but in a more flexible message format that transmits more Chip data.
- Generic EMV Transport

  This Card type is also EMV-Compliant but carries Issuer-defined online Chip information that is not processed by the Visa Europe System. VEAS treats Generic EMV Transport

transactions as **pass-through** transactions, valid for PIN translation but ineligible for field edit, Visa Chip or Issuer authentication services, or STIP.

VSDC requests for VIS and CCD Card types are eligible for PCAS processing and STIP. The following are Issuer-optional VEAS actions for a VSDC transaction when the Issuer has specified **route to Issuer** in the system tables:

- If PCAS parameters indicate **perform STIP**, VEAS sends the transaction to available Issuers
- If field 22 - POS Entry Mode Code contains code 05, 07, or 95, and the Issuer application data (IAD) in field 55 (tag 9F10) or in fields 134 or 135 exceeds 7 bytes for VIS Chip Card types (the total IAD length exceeds 7 bytes), or IAD bytes 19-32 do not equal binary zero for CCD Chip Card types, VEAS sends the transaction to available Issuers
- If Issuers are unavailable, VEAS reroutes the Chip Transactions to STIP, which applies Issuer-specified processing parameters

The Visa Europe System always sends Generic EMV Transport transactions to available Issuers or declines them in STIP if the Issuer is unavailable.

For further information about the VSDC Service, refer to the *Visa Europe Technical Service Descriptions*, and to the *Visa Smart Debit/Credit System Technical Manual*.

### B.22.1 VSDC PIN management service

The VSDC PIN Management Service allows Cardholders to change or to unblock PINs in VSDC Cards. Both Acquirers and Issuers must be certified participants in the service to provide the capability. Both must be VSDC-certified; Issuers must be full VSDC participants.

After the Cardholder enters the new PIN twice, the Acquirer forwards the new PIN in a **zero amount** 0100 Authorization Request to the Issuer for approval. Processing code 70 in field 3 - Processing Code indicates a PIN change; processing code 72 indicates a PIN unblock. The current PIN information is in field 52 - Personal Identification Number (PIN) Data and in field 53 - Security-Related Control Information; the new PIN is in field 152 - Secondary PIN Block. Approvals receive response code 85 (no reason to decline) in field 39 - Response Code. PIN change or unblock requests bypass activity checking and are not eligible for STIP. If the Issuer is unavailable or if the request times out, STIP responds with response code 91 in field 39.

VEAS does not include CVV or PIN Verification by the PVS with PIN management processing, only PIN translation. However, VSDC PIN Management Service participants may also participate in the PIN Verification Service and in the Card Verification Value (CVV) Service. For more information about the VSDC PIN Management Service, refer to the *Visa Europe Technical Service Descriptions*.

# C Visa Mandatory Minimum Limits

This appendix contains Visa mandatory minimum (MM) Issuer and activity limits.

## C.1 Visa-mandated Issuer limit and activity limit parameters

The following table contains the Visa-mandated Issuer limits and activity limits that Visa assigns to its Card products and Merchant Category Groups (MCGs). To understand Issuer limits and activity limits, refer to the following chapters in this book:

- Section 6.4, *Risk level and limits determination*: This section defines Issuer limits and describes their use as initial thresholds for routing transactions to Issuers or to STIP
- Chapter 8, *Stand-in processing (STIP)*: This chapter defines activity limits and describes how STIP uses them to approve or to decline transactions on behalf of Issuers

If the table does not list a particular Card product, then there are no mandatory minimum parameters for that particular product.

**Note** VEAS does not apply mandatory minimum Issuer or activity limits to debit or Prepaid Card transactions.

**Table 49: Visa-mandated limit parameters**

| Visa-mandated limit parameters | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Region and limits jurisdiction | Card product | Merchant Category Group | Issuer limit (USD) | 1-day activity limit | | 1-day activity limit count | | 4-day activity limit multiplier | |
| | | | | Issuer Available (USD) | Issuer Unavailable (USD) | Issuer Available | Issuer Unavailable | Issuer Available | Issuer Unavailable |
| 3 Visa Europe (VE) - International | Classic | 1 - Commercial Travel | 500.00 | 500.00 | 1,100.00 | 2 | 2 | 2.00 | 2.00 |
| | | 2 - Lodging | 500.00 | 500.00 | 900.00 | 2 | 2 | 2.00 | 2.00 |
| | | 3 - Auto Rental | 250.00 | 250.00 | 600.00 | 2 | 2 | 2.00 | 2.00 |
| | | 4 - Restaurant | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 5 - MOTO/e-commerce | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |

| Visa-mandated limit parameters | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Region and limits jurisdiction | Card product | Merchant Category Group | Issuer limit (USD) | 1-day activity limit | | 1-day activity limit count | | 4-day activity limit multiplier | |
| | | | | Issuer Available (USD) | Issuer Unavailable (USD) | Issuer Available | Issuer Unavailable | Issuer Available | Issuer Unavailable |
| | | 6 - Risky Purchase | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 7 - Other Purchase | 0.00 | 500.00 | 1,000.00 | 1 | 3 | 1.00 | 2.00 |
| | | 8 - Other Cash | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 9 - ATM Cash | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 10 - Quasi-Cash | 0.00 | n/a | n/a | n/a | n/a | 4.00 | 4.00 |
| | | 11 - Medical | 0.00 | n/a | n/a | n/a | n/a | 4.00 | 4.00 |
| 3 VE - International | Business | 1 - Commercial Travel | 750.00 | 750.00 | 2,200.00 | 2 | 2 | 2.00 | 2.00 |
| | | 2 - Lodging | 750.00 | 750.00 | 1,750.00 | 2 | 2 | 2.00 | 2.00 |
| | | 3 - Auto Rental | 350.00 | 350.00 | 900.00 | 2 | 2 | 2.00 | 2.00 |
| | | 4 - Restaurant | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 5 - MOTO/e-commerce | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 6 - Risky Purchase | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 7 - Other Purchase | 0.00 | 500.00 | 1,750.00 | 1 | 3 | 1.00 | 2.00 |

| Visa-mandated limit parameters | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Region and limits jurisdiction | Card product | Merchant Category Group | Issuer limit (USD) | 1-day activity limit | | 1-day activity limit count | | 4-day activity limit multiplier | |
| | | | | Issuer Available (USD) | Issuer Unavailable (USD) | Issuer Available | Issuer Unavailable | Issuer Available | Issuer Unavailable |
| | | 8 - Other Cash | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 9 - ATM Cash | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 10 - Quasi-Cash | 0.00 | n/a | n/a | n/a | n/a | 4.00 | 4.00 |
| | | 11 - Medical | 0.00 | n/a | n/a | n/a | n/a | 4.00 | 4.00 |
| 3 VE - International | Gold | 1 - Commercial Travel | 750.00 | 750.00 | 2,200.00 | 2 | 2 | 2.00 | 2.00 |
| | | 2 - Lodging | 750.00 | 750.00 | 1,750.00 | 2 | 2 | 2.00 | 2.00 |
| | | 3 - Auto Rental | 350.00 | 350.00 | 900.00 | 2 | 2 | 2.00 | 2.00 |
| | | 4 - Restaurant | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 5 - MOTO/e-commerce | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 6 - Risky Purchase | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 7 - Other Purchase | 0.00 | 500.00 | 1,750.00 | 1 | 3 | 1.00 | 2.00 |
| | | 8 - Other Cash | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |
| | | 9 - ATM Cash | 0.00 | 0.00 | 0.00 | 0 | 0 | 4.00 | 4.00 |

| Visa-mandated limit parameters | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Region and limits jurisdiction | Card product | Merchant Category Group | Issuer limit (USD) | 1-day activity limit | | 1-day activity limit count | | 4-day activity limit multiplier | |
| | | | | Issuer Available (USD) | Issuer Unavailable (USD) | Issuer Available | Issuer Unavailable | Issuer Available | Issuer Unavailable |
| | | 10 - Quasi-Cash | 0.00 | n/a | n/a | n/a | n/a | 4.00 | 4.00 |
| | | 11 - Medical | 0.00 | n/a | n/a | n/a | n/a | 4.00 | 4.00 |