BASE I Processing Specifications

V.I.P. SYSTEM

Effective: 1 Dec 2013

Important Note on Confidentiality and Copyright

The Visa Confidential label signifies that the information in this document is confidential and proprietary to Visa and is intended for use only by Visa Clients subject to the confidentiality restrictions in Visa's Operating Regulations, non-Client Third Party Processors that have an executed and valid Exhibit K on file with Visa, and other third parties that have a current nondisclosure agreement (NDA) with Visa that covers disclosure of the information contained herein.

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

Visa and other trademarks are trademarks or registered trademarks of Visa.

All other product names mentioned herein are the trademarks of their respective owners.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN: THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. VISA, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

If you have technical questions or questions regarding a Visa service or capability, contact your Visa representative. If you have comments or questions about this document, send them to TCS@visa.com.

Contents

CHAPTER 2 BASE I MESSAGES AND FLOWS

CHAPTER 4 BASE I LIMITS AND ROUTING

Figures

THIS PAGE INTENTIONALLY LEFT BLANK.

Tables

About This Manual

V.I.P. System BASE I Processing Specifications describes the processing requirements and options for the BASE I System component of the VisaNet Integrated Payment (V.I.P.) System. This manual provides an overview of BASE I and comprehensive information about BASE I message processing, including:

- Message types.
- Message flows for both authorization and non-authorization messages.
- Message editing.
- Message routing.
- Authorization limits.
- Stand-in processing (STIP).
- Reversals and advices.

This manual also describes BASE I user responsibilities and processing options and contains general information about the Cardholder Database and the Merchant Central File. These databases contain member-supplied data that BASE I uses to process transactions as members specify.

This manual is designed to be used with its companion, *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

AUDIENCE

V.I.P. System BASE I Processing Specifications is intended for members' technical staff and managers, as well as for Visa Member Services and customer support personnel who help members solve system and production problems.

STRUCTURE OF THIS MANUAL

V.I.P. System BASE I Processing Specifications is organized in six chapters.

Chapter 1, The BASE I System and the VisaNet Network—Provides an overview of BASE I processing functions and defines the scope of this manual. It also contains a basic overview of the V.I.P. System, including a description of VisaNet, VisaNet components, and V.I.P. transaction processing. It identifies and describes both BASE I *online* functions and *offline* functions. The chapter lists BASE I participation requirements and options both for acquirers and for issuers.

Chapter 2, BASE I Messages and Flows—Describes the differences between authorization and non-authorization messages. It also describes message editing, management, and routing, and provides message flow illustrations.

Chapter 3, Message Validation and Routing Preparation—Describes the initial processing that BASE I performs on messages it receives, including identifying the message types, validating their format, editing the message fields, determining issuer instructions and options, and logging the messages.

Chapter 4, BASE I Limits and Routing—Describes BASE I message routing in terms of the limits BASE I uses to determine whether to route the message to the issuer or to the stand-in processor (STIP). This chapter summarizes the routing services available to BASE I members, describing the ways that the Positive Authorization Capacity Management (PACM) Service, the Positive Cardholder Authorization Service (PCAS), and merchant category-related issuer limits control BASE I routing. The chapter defines merchant category groups (MCGs) and describes setting and using MCGs and issuer limits to provide full routing capabilities.

Chapter 5, Stand-In Processing (STIP)—Describes V.I.P. stand-in processing (STIP) from a BASE I perspective. It describes STIP functionality and defines the STIP selection hierarchy when it processes messages for issuers that have selected multiple limits, activity checking rules, exception file checking, card account number verification, and expiration date processing. This chapter also describes the effects of different advice limit and issuer limit combinations, mandatory minimum travel and entertainment (T&E) activity limits, cardholder risk-level activity thresholds, and random selection parameters. This chapter describes how PACM and PCAS function to enforce limits and which conditions trigger certain response codes.

Chapter 6, The BASE I Cardholder Database, Merchant Central File, and Advice File—Provides descriptions of the various files included in the Cardholder Database, their content, and member maintenance tasks. It also describes the Merchant Central File, which supplies information from acquirers to enhance messages at the terminal location.

Appendix A, Visa Mandatory Minimum Limits—Contains tables of Visa mandatory minimum issuer and activity limits.

DOCUMENT CONVENTIONS

Table 1 identifies the document conventions used in this manual.

Table 1 Document Conventions

Document Convention	Purpose in This Manual
boldface	Extra emphasis (stronger than italics); field values and codes.
EXAMPLE	Identifies an example of what the accompanying text describes or explains.
IMPORTANT	Highlights important information in the text.
italics	Document titles; emphasis; variables; terms or acronyms being defined.
“text in quote marks”	Section names referenced in a chapter; first instance of a word used in an unconventional or technical context.
`text in Courier New font`	URLs and email addresses.
NOTE	Provides more information about the preceding topic.
n/a	Not applicable.
shaded illustrations	Systems or procedures that are not directly involved in the process being illustrated in the graphic.

Table 1 Document Conventions (continued)

Document Convention	Purpose in This Manual
white boxes in flow diagrams	White boxes represent request messages.
shaded boxes in flow diagrams	Shaded boxes represent response messages.
dotted line boxes in flow diagrams	Boxes with dotted lines illustrate advice messages.

SYSTEM DOCUMENTATION DESCRIPTIONS

The first three manuals in this series: *V.I.P. System Overview*, *V.I.P. System Services, Volume 1 and Volume 2*, and *V.I.P. System Reports*, apply both to BASE I System processing and to Single Message System (SMS) processing.

The next two manuals are specific to the BASE I System: *V.I.P. System BASE I Processing Specifications* and *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

For the Single Message System (SMS), the Visa U.S.A. (U.S.) region processing specifications for ATM, for Interlink, and for POS are consolidated in one manual, *V.I.P. System SMS Processing Specifications (U.S.)*. For the international audience, there are separate processing specifications manuals for ATM and for POS.

This manual contains new and updated information, and incorporates all system changes and revisions described in the October 2013 VisaNet Business Enhancements Global Technical Letters and Implementation Guides published after April 2013 through October 2013.

Table 2 provides brief descriptions of the V.I.P. System manuals.

Table 2 Descriptions of V.I.P. System Manuals

General Information
V.I.P. System Overview Provides basic descriptions of the VisaNet network and its components, access points, processing concepts, requirements, and options. Contains descriptions of the V.I.P. System, the BASE I System, and the Single Message System (SMS), VisaNet Access Points (VAPs), issuer and acquirer responsibilities, and Visa Interchange Center (VIC) operations. Also provides a brief introduction to V.I.P. services. Doc ID 0851-22
V.I.P. System Reports Provides sample reports for BASE I and SMS processing and for V.I.P. System services. Doc ID 0852-22

About This Manual

Table 2 Descriptions of V.I.P. System Manuals (continued)

V.I.P. System Services, Volume 1

Provides complete information about V.I.P. System services available to BASE I users and to SMS users. Service descriptions include basic information, processing requirements, options, features, key message fields, and message flows.

Volume 1 contains the following parts:

Part 1: V.I.P. Basics
Part 2: Routing Services
Part 3: Risk Management Services
Part 4: Visa Secure Electronic Commerce (VSEC) Services
Part 5: Chip Card Services

Doc ID 0853A-22

V.I.P. System Services, Volume 2

Provides complete information about V.I.P. System services available to BASE I users and to SMS users. Service descriptions include basic information, processing requirements, options, features, key message fields, and message flows.

Volume 2 contains the following parts:

Part 6: Authorization Database Files and Services
Part 7: Authorization Services

Doc ID 0853B-22

Table 2 Descriptions of V.I.P. System Manuals (continued)

BASE I
V.I.P. System BASE I Processing Specifications Describes V.I.P. transaction processing in the BASE I System environment, including message types, processing considerations, related services, and VisaNet Access Points (VAPs). Doc ID 0847-22
V.I.P. System BASE I Technical Specifications, Volume 1 Documents technical specifications of V.I.P. transaction processing in the BASE I System environment. This companion volume to *V.I.P. System BASE I Processing Specifications* describes the fields for BASE I. Doc ID 0844A-23
V.I.P. System BASE I Technical Specifications, Volume 2 Documents technical specifications of V.I.P. transaction processing in the BASE I System environment. This companion volume to *V.I.P. System BASE I Processing Specifications* describes the message formats and the file specifications for BASE I. Doc ID 0844B-23
Interlink
V.I.P. System SMS Processing Specifications (U.S.) Contains information about the Single Message System, including message types, processing considerations, VisaNet Access Points (VAPs), and related services for Interlink, Visa and Plus ATM, Visa POS, and Visa Electron. Doc ID 0857-22
V.I.P. System SMS Interlink Technical Specifications Companion volume to *V.I.P. System SMS Processing Specifications (U.S.)*. Describes message formats, field descriptions, and file specifications for Interlink. Doc ID 0866-21
SMS ATM
V.I.P. System SMS Processing Specifications (U.S.) Contains information about the Single Message System, including message types, processing considerations, VisaNet Access Points (VAPs), and related services for Visa and Plus ATM, Interlink, Visa POS, and Visa Electron for members in the Visa U.S.A. (U.S.) region. Doc ID 0857-22
V.I.P. System International SMS ATM Processing Specifications Contains information about Single Message System ATM processing, including message types, processing considerations, VisaNet Access Points (VAPs), and related services for members outside of the U.S. region. Doc ID 0839-22

Table 2 Descriptions of V.I.P. System Manuals (continued)

V.I.P. System SMS ATM Technical Specifications, Volume 1

Companion volume to *V.I.P. System SMS Processing Specifications (U.S.)* and to *V.I.P. System International SMS ATM Processing Specifications*. Contains information about field descriptions for ATM.

Doc ID 0868A-21

V.I.P. System SMS ATM Technical Specifications, Volume 2

Companion volume to *V.I.P. System SMS Processing Specifications (U.S.)* and to *V.I.P. System International SMS ATM Processing Specifications*. Contains information about message formats and file specifications for ATM.

Doc ID 0868B-21

SMS POS

V.I.P. System SMS Processing Specifications (U.S.)

Contains information about the Single Message System, including message types, processing considerations, VisaNet Access Points (VAPs) and related services for Visa POS, Visa Electron, Visa and Plus ATM, and Interlink for members in the U.S. region.

Doc ID 0857-22

V.I.P. System International SMS POS (Visa & Visa Electron) Processing Specifications

Contains information about Single Message System POS processing, including message types, processing considerations, VisaNet Access Points (VAPs), related services, and reports for members outside of the U.S. region.

Doc ID 0835-22

V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1

Companion volume to *V.I.P. System SMS Processing Specifications (U.S.)* and to *V.I.P. System International SMS POS (Visa & Visa Electron) Processing Specifications*. Describes the fields for Visa POS and for Visa Electron.

Doc ID 0869A-21

V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 2

Companion volume to *V.I.P. System SMS Processing Specifications (U.S.)* and to *V.I.P. System International SMS POS (Visa & Visa Electron) Processing Specifications*. Describes message formats and file specifications for Visa POS and for Visa Electron.

Doc ID 0869B-21

SOURCES OF SYSTEM INFORMATION

This section lists the primary sources for the information contained in *V.I.P. System BASE I Processing Specifications*. The information from these sources has been analyzed, rewritten, and reorganized, when necessary. Technical staff and subject matter experts reviewed and verified these updates. In addition, this revised manual incorporates, where appropriate, all of the comments and change requests received from members and from Visa staff.

Existing V.I.P. System Manuals

For a list of the existing V.I.P. manuals, refer to Table 2.

VisaNet Business Enhancements Global Technical Letters and Implementation Guides

The *V.I.P. System BASE I Processing Specifications* includes information from the following technical letter and implementation guide: the October 2013 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Version 3.0, effective 19 September 2013.

OBTAINING REPORT SAMPLES

Visa offers several reports to members. Many of these reports clarify and track service processing. The following manuals provide report samples:

- *V.I.P. System Reports*
- *VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports*

Members can contact their Visa representatives to discuss reporting options or to obtain additional report samples.

FOR MORE INFORMATION

Visa provides documentation to support Visa products and services. For many of the services described in this manual, Visa has developed implementation guides that contain region-specific details about signing up for a service, selecting options, and installing, testing, and operating the service. Members can ask their Visa representatives for regional guides.

The V.I.P. documentation suite does not contain details about the BASE II System. For information about this system, members can contact their Visa representatives.

Related Publications

The publications listed in this section provide information about Visa systems, regulations, and additional services not covered in this manual. If you have technical questions or questions regarding a Visa service or capability, contact your Visa representative.

Use the following information to obtain any of the listed publications, to be added to or removed from distribution lists, or to inquire about other publications.

- U.S. members and third-party processors can contact Publication Orders by sending an email to publicationorders@visa.com.
- Members and third-party processors in all other Visa regions or in Miami can contact their Visa representatives.

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

Operating Regulations

The operating regulations are contained in the *Visa International Operating Regulations (VIOR)*.

Qualifying merchants and third-party agents can also request a copy of the *Interchange Qualification Guide*.

Deferred Clearing Advice File (DCAF) Service

For information about the DCAF Service, refer to *V.I.P. System Services, Volume 2*.

PIN Management Requirements

For complete, current information about PIN management requirements, refer to:

Payment Card Industry PIN Security Requirements Manual—This manual contains requirements for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and at attended and unattended terminals.

PIN-Entry Device Security Requirements—The following manuals contain physical and logical security device requirements and management procedures for online and offline PIN-entry devices and the procedures and forms that entities use to measure compliance:

- *Payment Card Industry Encrypting PIN PAD (EPP) Security Requirements Manual*
- *Payment Card Industry POS PIN-Entry Device Security Requirements Manual*

POS Check Service

For information about the POS Check Service, refer to:

Visa U.S.A. POS Check Service Operating Regulations

V.I.P. System Services, Volume 2

V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1 and Volume 2

VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports

Risk Management Services

For information about risk management services, refer to:

Card Recovery Bulletin Service User's Guide

Fraud Reporting System (FRS) User's Guide

Issuer's Clearinghouse Service User's Guide

Merchant Fraud Performance Program Guide

Risk Management Process Guide

V.I.P. System Services, Volume 1

Visa Risk Manager

Security

For complete, current information about data and system security, refer to:

Payment Technology Standards Manual—This manual contains standards for PINs and for encoding account and cardholder data on Visa payment form factors.

Visa Extended Access Servers (EA Servers)

For information about Visa Extended Access Servers (EA Servers), refer to:

Extended Access Administration and Installation Guide

Visa Extended Access Server Endpoint Guide

Extended Access Management Installation Guide

Extended Access Management Operators Guide

Extended Access Security Administration Guide

Extended Access Server Endpoint Guide

Visa Incentive Network (VIN)

For information about the Visa Incentive Network (VIN), refer to:

Visa Incentive Network Service Description—(This is a high-level overview and is not the same as the *V.I.P. System Services* descriptions.)

Visa Incentive Network Member Implementation Guide

Credit Rewards Key Implementation Tasks and Best Practices

Credit Rewards: Visa Incentive Network and Credit Interchange Frequently Asked Questions

October 2005 VisaNet Business Enhancements Technical Letter, updated version 3.0, dated September 15, 2005

Visa Traditional Rewards Registration Toolkit

Visa Signature Registration Toolkit

Visa Resolve Online (VROL)

For information about Visa Resolve Online (VROL), refer to:

Visa Resolve Online Administrator's Guide

Visa Resolve Online Bulk Systems Interface Development Guide

Visa Resolve Online Member Implementation Guide

Visa Resolve Online Real-Time Systems Interface Development Guide

Visa Resolve Online Reference Manual

Visa Resolve Online User's Guide

Visa Smart Debit/Smart Credit (VSDC) Service

For information about the VSDC Service, refer to:

V.I.P. System Services, Volume 1—This manual contains a complete service description.

JCB, MasterCard, Visa (EMV) Specifications, EMV '96 Version 3.1.1 and EMV 2000 Version 4.0—These documents contain industry standards for chip card and terminal interaction. They are available at `www.emvco.com`.

Visa Smart Debit and Visa Smart Credit Service Description—This manual provides a high-level description of the features and the benefits of a VSDC program.

Visa Smart Debit and Credit Planning Guide—This manual helps members plan their VSDC program and migration strategy to position themselves competitively for the future.

Visa Smart Debit and Credit Member Implementation Guide for Acquirers—This manual provides guidelines for acquirers involved in the implementation of new VSDC programs.

Visa Smart Debit and Credit Member Implementation Guide for Issuers—This manual provides guidelines for issuers involved in the implementation of new VSDC programs.

Visa Smart Debit/Visa Smart Credit System Technical Manual—This manual provides information for members and for Visa staff responsible for the implementation and the operation of a VSDC program.

Visa Integrated Circuit Card Specifications (VIS)—This 3-volume manual contains the technical specifications for the VSDC card application, describing both the functionality and the flow of a VSDC transaction.

Miscellaneous Systems and Services

For more information about miscellaneous systems and services relevant to V.I.P., refer to:

Credit Gateway Service Cross-Reference Guide—This document includes field-by-field data transfer descriptions between V.I.P.-format dual-message transactions, and American Express- and MasterCard-format transactions.

V.I.P. System Services, Volume 1 and Volume 2

For More Information

Visa Global ATM Planning Guide—This manual contains information about the Visa and Plus International ATM Program. It includes an overview of the program, its business requirements, optional services, risk management, processing options, testing procedures, and back-office management.

Visa Information System User's Guide

Visa Test System—V.I.P. User's Guide

VisaNet Settlement Service (VSS) User's Guide, Volume 1, Specifications

VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 1 The BASE I System and the VisaNet Network

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

- A brief description of the VisaNet network and its major systems.
- An overview of BASE I participation requirements and BASE I functions.

A complete overview of VisaNet and of the V.I.P. System can be found in the *V.I.P. System Overview*.

1.1 THE VISANET NETWORK

VisaNet is the Visa transaction processing network, the structure that supports transactions routed among acquirers and issuers in all Visa regions. The term *VisaNet* applies to the network's hardware, software, and communications components and facilities, as well as member regional systems and networks.

The main components of VisaNet are:

- VisaNet Interchange Centers (VICs).
- VisaNet Communications Network.
- VisaNet Access Points (VAPs), such as Direct Exchange (DEX), and Visa Extended Access Servers (EA Servers).

NOTE

Members in the Visa U.S.A. (U.S.) region access VisaNet through DEX. Members in all other Visa regions currently access VisaNet through DEX or EA Servers.

- Processing Centers.

VisaNet Interchange Centers (VICs)—A *VIC* is a Visa data processing center. Each VIC houses the computer systems that perform all VisaNet transaction processing and serves as the control point for the telecommunications facilities of the VisaNet Communications Network. VisaNet connects members to the closest VIC. If one VIC experiences system disturbances that interrupt system processing, VisaNet automatically routes members' transactions to another VIC, ensuring continuity of service.

Each VIC houses BASE I as a component of the *VisaNet Integrated Payment (V.I.P.) System*, the main Visa transaction processing system. Two of the VICs house the Single Message System (SMS) as a software component of V.I.P.

VisaNet Communications Network—Visa operates telecommunications lines and facilities worldwide to link all systems users to the VICs and thus to each other. Most links in the VisaNet 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.

VisaNet Access Points—Visa provides access points for connecting to VisaNet. These VisaNet Access Points (VAPs) enable members to connect to VisaNet for transaction processing. VAPs include:

- Direct Exchange (DEX)

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

  The network has two major components:

  - The *Visa Message Gateway*, which handles online transaction processing, resides at the VIC and supports all V.I.P. messages. The Visa Message Gateway operates as a routing “switch” for all V.I.P. transactions processed through it, controls the flow of traffic between access points and the VIC, and effectively replaces VAPs in end-to-end BASE I 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, BASE II data, the Point-of-Sale Authorization (POSA) File, and various reports and raw data.

- Visa Extended Access Servers (EA Servers)

  EA Servers are based on open systems technology and on a hardened Solaris operating system. EA Servers are located at participating access point sites. The servers perform authorization routing, file staging, and delivery services, and provide secure connectivity to VisaNet.

  EA Servers allow accessibility and flexibility, thereby enabling easy deployment for future Visa product and service offerings, as well as other customization. Their modular interface adapts to front-end systems and integrates standard, off-the-shelf components that members can scale to meet specific service needs.

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

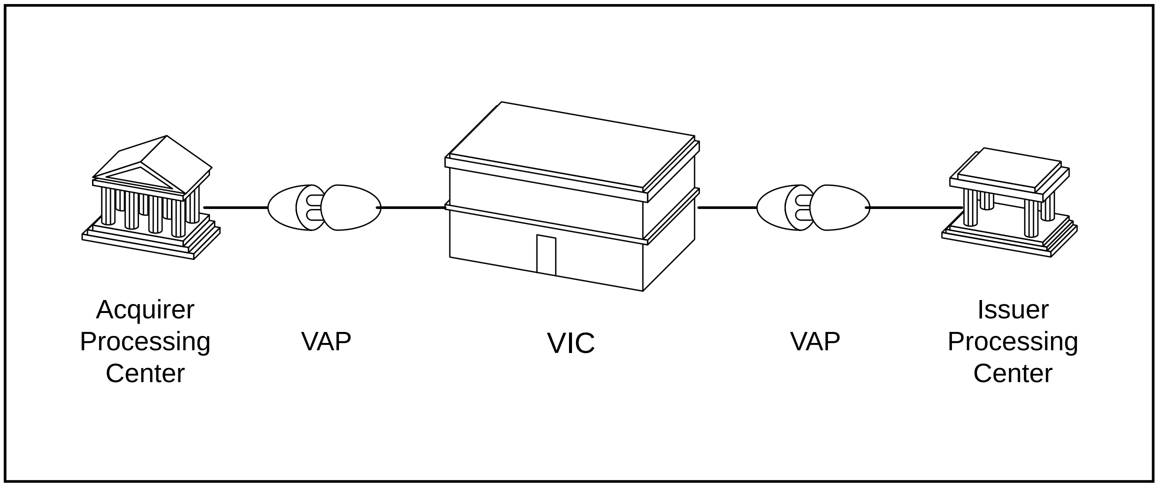
Options vary by region. Members can contact their Visa representatives for information about available connectivity options.

Refer to “For More Information” in About This Manual for documentation about VisaNet connections.

Processing Center—A *processing center*, often called a *processor*, is a data processing facility operated by or designated by an issuer or an acquirer. The processing center houses card processing systems that support merchant and business locations, maintain cardholder data and billing systems, or both. Each processing center host computer that communicates with a VAP must run a computer interface to the VAP. Visa must test this interface before the VAP can be connected to VisaNet.

Figure 1-1 illustrates the traditional VisaNet network, with VisaNet Access Points (VAPs) in place. The BASE I System is a subset of the V.I.P. System, which is part of VisaNet.

Figure 1-1 The VisaNet Communications Network



1.2 VISANET SYSTEMS

There are three main transaction processing systems within VisaNet that provide online and offline transaction processing:

- The VisaNet Integrated Payment (V.I.P.) System, which includes:
  - The BASE I System
  - The Single Message System (SMS)
- The BASE II System
- The VisaNet Settlement Service (VSS)

The following subsections describe each of these VisaNet systems.

1.2.1 VisaNet Integrated Payment (V.I.P.) System

The *V.I.P. System* is the primary online transaction routing (switching) and processing system for all online authorization and financial request transactions that enter VisaNet. The system provides the V.I.P. services described in this manual to members and to other users worldwide.

V.I.P. 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 interchange card transactions that contain both authorization and clearing information in a single message). In both cases, settlement occurs separately.

1.2.2 BASE I System

BASE I is the component of the V.I.P. System that processes authorization-only request messages online. *Authorization request messages* are the first messages sent in dual-message processing. (*BASE II clearing messages* are the second messages sent in dual-message processing.)

The BASE I component of the V.I.P. System supports online functions, offline functions, and the BASE I files. BASE I files include the internal system tables and the Merchant Central File (MCF).

Refer to *V.I.P. System Services, Volume 2*, for information about the Merchant Central File.

BASE I Online Functions—The BASE I *online* functions support dual-message authorization processing. BASE I online processing involves routing, cardholder and card verification, and stand-in processing (STIP), plus related functions, such as Card Verification Value (CVV) validation, PIN verification, and file maintenance.

> **NOTE**
>
> *BASE I processes U.S. domestic Interlink-acquired transactions if the account range is set up to accept PIN-authenticated POS transactions.*

A bridge from BASE I to SMS makes it possible for BASE I members to communicate with SMS members and to access the SMS gateways to outside networks.

Refer to *V.I.P. System Services, Volume 1*, for information about networks supported by Gateway Services.

How BASE I routes and processes a transaction depends on:

- The type of card used.
- The processing network preferred by the acquirer.
- The type of acquirer, BASE I—Issuer either BASE I or SMS.
- The type of message used to request processing of the transaction, either authorization or financial.
- The type of issuer processing center, BASE I—Acquirer either BASE 1 or SMS.

For each card transaction, BASE I supports authorizations using either:

- BASE I processing rules ***or***
- V.I.P. processing rules

The member's choice of processing options affects whether BASE I processes the transaction according to BASE I rules or to V.I.P. rules. Refer to “BASE I Participation Requirements” in this chapter for information about establishing BASE I connections and about the options that are available.

Depending on the processing rules and on the type of transaction, BASE I 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, U.S. bill payment, partial authorization, recurring payment, installment payment, or contactless) purchase transactions, and cash transactions (ATM, manual cash, and quasi-cash).
  - Visa Smart Debit/Smart 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

    VisaNet does not provide stand-in processing for MasterCard transactions.

  - American Express authorizations, partial authorizations, and balance returns.
  - American Express, Diners Club International, and Discover International purchase transactions.

    NOTE

    VisaNet does not provide stand-in processing for Diners Club International transactions. It does provide limited stand-in processing for Discover International transactions and for American Express transactions.

    NOTE

    When VisaNet receives Diners Club International (DCI) 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 (DCI) products are separate products and VisaNet 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.

- Check Acceptance Service requests for U.S.-region-only merchants using Equifax Card Services (TeleCredit Los Angeles and TeleCredit Tampa), ETC Scan (Deluxe Data Systems), JBS/NPC, State Street Bank, or TeleCheck.
- Address verification for authorization requests when the acquirer requests verification and participates in the Address Verification Service (AVS).

NOTE

When V.I.P. receives an AVS-only account verification request destined for a U.K. issuer that is directly connected to Visa Europe Authorisation Services, V.I.P. forwards the request to Visa Europe Authorisation Services, which determines whether the request is to be processed by its stand-in processing system or forwarded to the issuer.

- Reversals of previously approved transactions.
- File updates and inquiries.

IMPORTANT

BASE I processes Interlink-acquired preauthorization request messages if they are U.S. domestic and the account range is set up to process PIN-authenticated POS transactions.

Floor Limit Considerations

A merchant's *floor limit* is an amount limit set by the acquirer (subject to *Visa International Operating Regulations* maximums) that determines if the transaction requires V.I.P. authorization for completion. BASE I only processes transactions above a merchant's floor limit. Transactions at or below the floor limit do not require authorization processing.

IMPORTANT

Merchants 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 minimize members' risk. Refer to the *Visa International Operating Regulations* for details. Refer also to releases of VisaNet Global Business Enhancements documents (and to their update bulletins) for floor limit changes that occur between releases of *Visa International Operating Regulations (VIOR)*.

BASE I Offline Functions—The BASE I *offline* functions include BASE I reporting and the generation of Visa Card Recovery Bulletins. BASE I reporting includes authorization reports, Exception File and Advice File reports, and POS reports. For more information about BASE I offline functions, refer to "Online Functions" in this chapter.

1.2.3 Single Message System (SMS)

The *Single Message System (SMS)* component of the V.I.P. System 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

BASE I, and accessing outside networks, as required, to complete transaction processing. ***Only*** the SMS component performs single-message processing.

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

Refer to *V.I.P. System Services, Volume 1*, for information about networks supported by Gateway Services.

SMS supports online functions, offline functions, and SMS files. SMS files consist of internal system tables that control system access and processing. SMS also supports the Merchant Central File for SMS members in the U.S. region.

SMS Online Functions—The SMS *online* functions perform real-time cardholder transaction processing and exception processing. This processing supports authorization *and* full financial transactions. In addition, SMS supports the delivery of transactions to the BASE II System for members that use dual-message processing.

SMS also accumulates reconciliation totals, performs activity reporting, and passes activity data to VisaNet, which supports settlement and funds transfer processing for SMS. VisaNet handles settlement and funds transfer as an automatic follow-up to SMS transaction processing. The *VisaNet Settlement Service (VSS)* performs settlement as a separate process and delivers its results through advices and reports. For an illustration of the relationship of VSS to SMS and to BASE II, see "VisaNet Settlement Service (VSS)" in this chapter.

Issuers can choose to have all of their transactions processed by SMS or can use BASE I and BASE II, as well as SMS, to process their transactions. Issuers can also choose to use different processing methods for different Visa products.

SMS Offline Functions—The SMS *offline* systems process settlement and funds transfer requests and provide settlement and activity reporting. (SMS members may also receive the BASE I reports mentioned in "BASE I Offline functions" in this chapter.) The offline systems also support an offline bridge to and from BASE II for those Visa and Plus clearing transactions that VisaNet sends between an SMS member and a BASE II member.

V.I.P. System BASE I Processing Specifications describes only the aspects of SMS that pertain to BASE I transactions and processing. Refer to About This Manual for a complete list of SMS manuals.

1.2.4 BASE II System

The *BASE II System* is an international electronic batch transaction clearing system that facilitates the exchange of interchange data between acquirers and issuers. The system calculates interchange fees between members.

BASE II performs the second part of dual-message processing. Through a BASE I or SMS connection, members submit authorization messages, which V.I.P. clears through a VisaNet connection to BASE II. A bridge to the V.I.P. System permits interchange between BASE II processing centers and SMS processing centers.

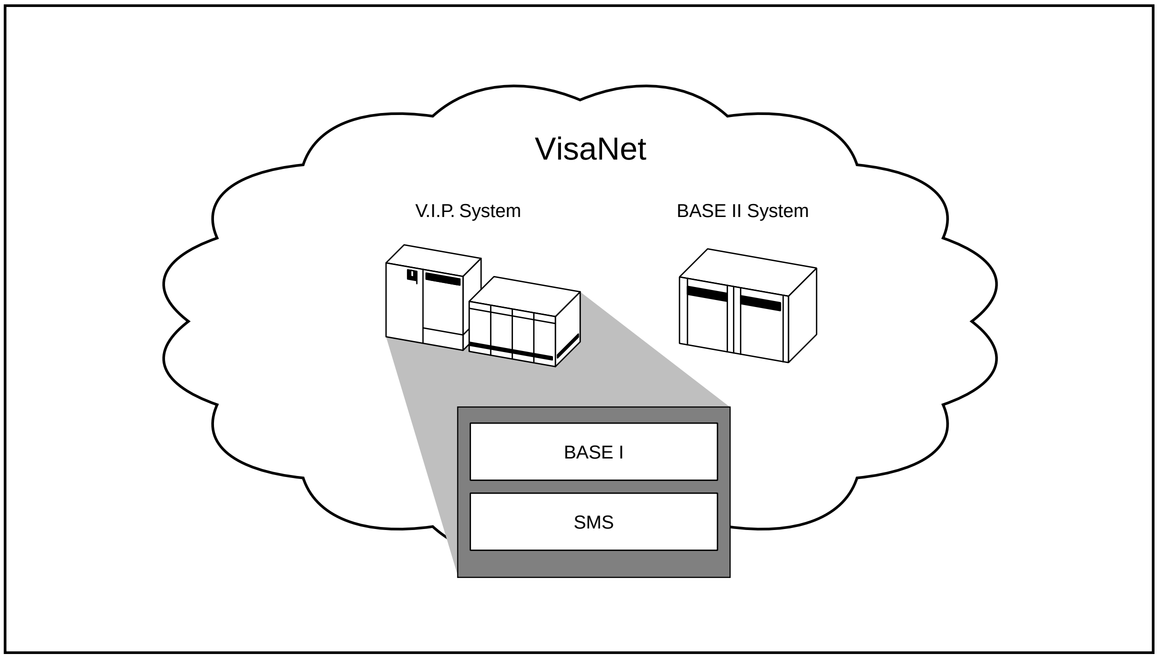
NOTE

This manual does not provide details about BASE II. For information about this system, members can contact their Visa representatives.

Settlement occurs through VSS. BASE II passes message data to VSS, which settles with the issuer and with the acquirer. For information about VSS, see "VisaNet Settlement Service (VSS)" in this chapter.

The following figure illustrates where V.I.P. and its software system components, along with BASE II, reside in the VisaNet network.

Figure 1-2 The VisaNet Software System Components



Visa members and processors that use BASE I and BASE II 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 BASE I and BASE II processing for POS transactions and use SMS processing for ATM transactions.

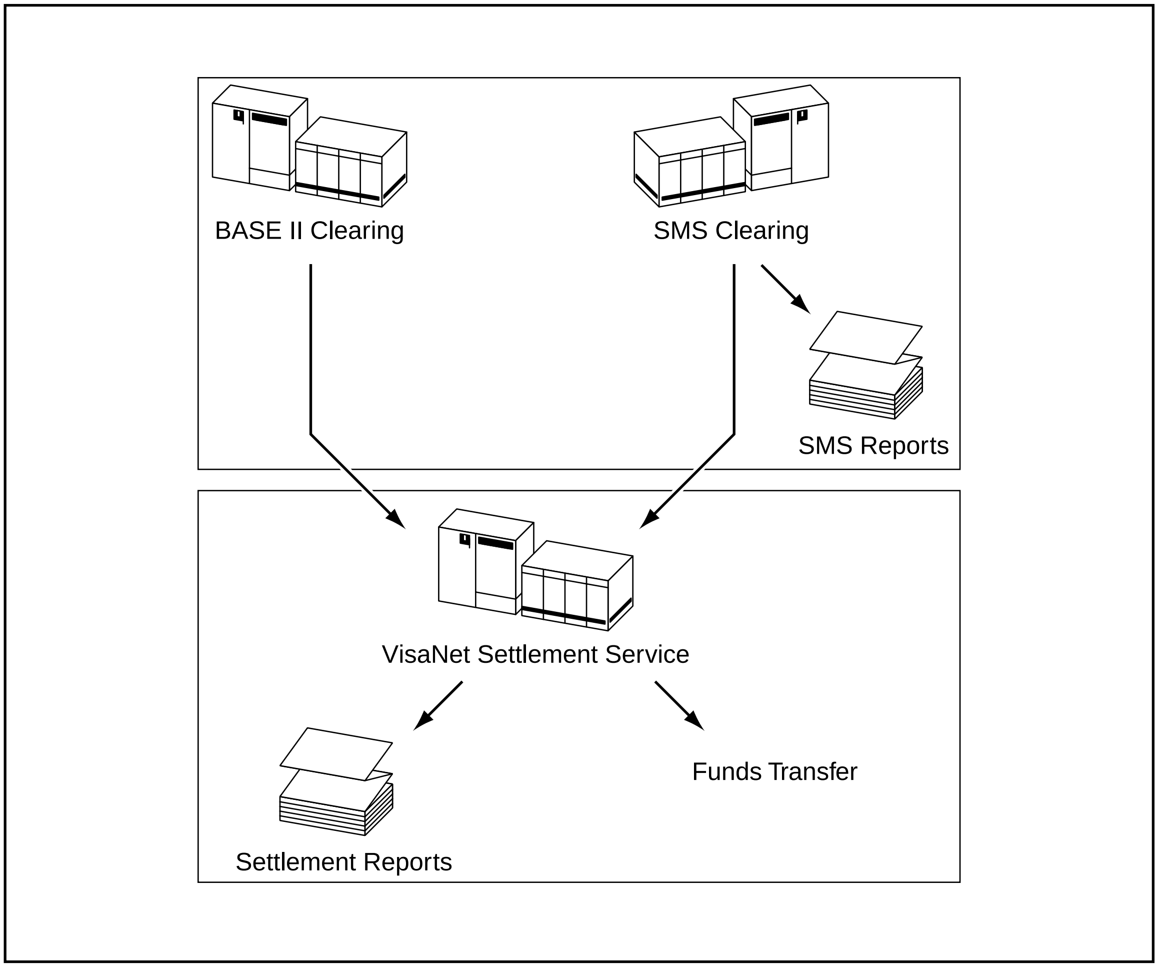
1.2.5 VisaNet Settlement Service (VSS)

VisaNet processes interchange transactions for SMS and for BASE II through separate systems. Both SMS and BASE II 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* has two components: The first component is the process of calculating and determining the net financial position of each member for all the transactions cleared by VisaNet. The second component is the process during which actual exchange of funds takes place.

The *VisaNet Settlement Service (VSS)* consolidates the settlement functions of SMS and BASE II, including Interlink and Plus, into a single service for all products and services. VisaNet sends the settlement information to members and processors from SMS and from BASE II in a standardized set of reports. VSS provides flexibility in defining financial relationships, in selecting reports and report destinations, and in establishing funds transfer points.

Figure 1-3 illustrates the VSS clearing and settlement process.

Figure 1-3 VisaNet Settlement Service (VSS) Process



1.3 THE COMMON MEMBER INTERFACE (CMI) AND OTHER INTERFACE METHODS

The *Common Member Interface (CMI)* is an interface method that allows members and processing centers to use the same communications line to send and to receive BASE I and SMS messages. The communications line from a VisaNet access point, or station, to V.I.P. connects at the CMI at the VIC.

NOTE

Members establish processing and routing parameters for their stations in the system tables through the Customer Online Repository (CORE). Members can contact their Visa representatives to establish or to change their CORE settings.

The CMI accepts messages in all valid message formats. Functions of the CMI include basic editing as well as routing.

With the CMI, any BASE I processing center, including those that use both BASE I and SMS, can send BASE I messages. Any SMS processing center, including those that use both SMS and BASE I, can send SMS messages. The CMI chooses the appropriate system based on the source of the request, on the type of processing requested, and on the processing network in cases when the message specifies a network.

Besides the CMI, other interface methods are available to members and to processing centers. These methods allow members and processing centers to communicate with *only one* component of V.I.P.—with BASE I or with SMS but not with both.

1.4 BASE I PARTICIPATION REQUIREMENTS

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

VisaNet members that choose BASE I processing must fulfill all of the BASE I participation requirements. These requirements can vary, depending on whether the member is a BASE I issuer or acquirer and on which access devices and processing options the member selects.

Members connecting to BASE I must consider:

- VisaNet access devices.
- Processing options and parameters.
- Message support requirements.

The following section identifies basic system requirements, options, and parameters for acquirers and for issuers. Members can contact their Visa representatives for complete requirements, available options, and help in establishing parameters.

IMPORTANT

Visa has adopted the industry-standard Triple Data Encryption Standard (TDES). This change applies to all Visa members and covers all PIN-based Visa credit and debit, Interlink, and Plus transactions processed through VisaNet. All VisaNet endpoints must use TDES Issuer Working Keys (IWKs) and Acquirer Working Keys (AWKs).

1.4.1 VisaNet Access Devices

Acquirers and issuers determine optimal VAP 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 BASE I and SMS processing center may use a single VAP for both BASE I and SMS messages, or it may use separate BASE I and SMS VAPs. The choice depends on the center's system configuration.

- Separate host computers for BASE I and for SMS processing require separate VisaNet access devices.
- A single host may be configured with one or with two VisaNet access devices.

VAP interface requirements depend on the type of device selected. Refer to About This Manual for a list of VAP manuals.

1.4.2 BASE I Processing Options and Parameters

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

Members connected to BASE I must select the processing options best suited to their regions and to the types of transaction traffic they support. Services and processing options include those applicable at the BIN level, at the processing center level, at the individual processing center station level, and, in the U.S. region and in Visa Canada, at the card level.

1.4.2.1 Acquirer Considerations

Acquirers must determine their policies for the BASE I processing of their transactions. Issuers must establish parameters for message response times and must determine the actions that BASE I is to take when they fail to respond within the prescribed time.

Adequate time must be allowed for issuer centers to respond, but issuers, in turn, must be responsive to the time-out demands of their electronic terminals and ATMs. To be approved by Visa, they *must* support timed-out transactions. If an acquirer experiences a time-out, it *must* do one of the following:

Retry the transaction—If the merchant or the acquirer decides to retry the transaction, it *must* send a reversal of the original request or a repeat of the original request. Visa recommends sending both a reversal ***and*** a repeat.

Reverse the transaction—If the merchant or 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 V.I.P., 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 because V.I.P. rejects the reversal request if field 38 is not present with Reject Code **0293**—Field 38 Missing.*

Refer to “How V.I.P. Processes Repeat, or Duplicate, Authorization Requests” in Chapter 3 for further information about timed-out messages.

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.

1.4.2.2 Issuer Considerations

Issuers must establish in-house processing centers or must designate other processing centers or third-party processors to perform the necessary issuer and cardholder functions.

Issuers must also establish parameters (limits) for BASE I to use when it makes routing and STIP authorization decisions. There are three main types of limits: issuer limits, advice limits, and activity limits. Refer to Chapter 4, BASE I Limits and Routing, and to Chapter 5, Stand-In Processing (STIP), for detailed information about these and other parameters. V.I.P. stores the limits in the system tables (formerly called the *system globals*) and in the Cardholder Database. Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for information about this database.

1.4.3 Message Support Requirements for Acquirers and for Issuers

Issuers and acquirers must fulfill all BASE I 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 BASE I request when it is not available from the point of sale or point of service (POS). Members can optionally use the Merchant Central File Service (MCFS) for this task. VisaNet requires access for updating the files maintained at the VIC only if the center uses MCFS. Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, in this manual as well as to *V.I.P. System Services, Volume 2*, for information about MCFS.
- The ability to manage all of the messages related to any given customer 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, for instance, the Address Verification Service (AVS), the PIN Verification Service (PVS), or MCFS. Refer to *V.I.P. System Services, Volume 1 and Volume 2*, for complete information about services provided by V.I.P.
- Downtime procedures and appropriate recovery.

Members can contact their Visa representatives for complete information about full support requirements for BASE I messages.

1.4.3.1 Message Format

BASE I and SMS members use the V.I.P. message format.Refer to Chapter 2, BASE I Messages and Flows, for further description of the V.I.P. message format.

1.4.3.2 Testing

Visa must test that member centers can process messages before they can use the V.I.P. System. Members can contact their Visa representatives for complete information about testing.

1.4.3.3 Additional Message Processing Procedures for Acquirers

BASE I acquirers must ensure that their card processing systems are capable of generating and of receiving all of the various VisaNet messages necessary for the types of card processing the centers 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 instance. acquirers must convey a card pick-up request to a merchant explicitly, not as a simple decline.
- 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.
- Establish procedures to handle non-routine responses from the issuer, such as BASE I referrals or Interlink or American Express partial approvals, as applicable.
- Support reversal messages. BASE I centers use reversals to cancel previously approved transactions.

1.4.3.4 Issuer and Acquirer Reversal Processing Requirements

This section describes the processing practices that acquirers and issuers must follow to send and to receive reversals.

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, not in 0400 financial reversals. An 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. Because the acquirer did not receive an authorization response from V.I.P., 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 because V.I.P. rejects the authorization reversal request if field 38 is not present with Reject Code **293**—Field 38 Missing.

Refer to “How V.I.P. Processes Repeat, or Duplicate, Authorization Requests” in Chapter 3 for further information about timed-out messages.

Processing of Multiple Partial Reversals

BASE I does not retain message data from previous reversals. BASE I 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 “Activity Testing on Reversals” in Chapter 5, Stand-In Processing (STIP), for more information about reversal processing and about activity checking.

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.

NOTE

BASE I does not maintain transaction histories after VisaNet or the issuer sends a response. Therefore, BASE I cannot match reversals to originals, and cannot always approve reversals processed by STIP.

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.

1.4.4 Resolving Transaction Failures

Occasionally, member-initiated transactions fail to process as anticipated; for instance, V.I.P. might reject a request because of an invalid field value. Member representatives can help resolve such problems.

1.4.4.1 The Role of V.I.P. Member Representatives

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

- The time and date of the occurrence. Support staff prefers an exact time but accepts a limited time range.
- Transaction details, for instance, credit, SMS, or both, region, PCR, station, and BIN.
- The circumstances surrounding the issue, for instance, 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 instance, 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 dollar amounts of the transactions.

With the above items in hand, the support teams can start analyzing the situation immediately instead of spending time gathering the information first.

To resolve these events as quickly as possible, Visa member representatives should be contacted.

NOTE

Unless Full Logging is turned on at the BASE I station or PCR level, V.I.P. logs only the IO segment for 0110 responses to credit transactions.

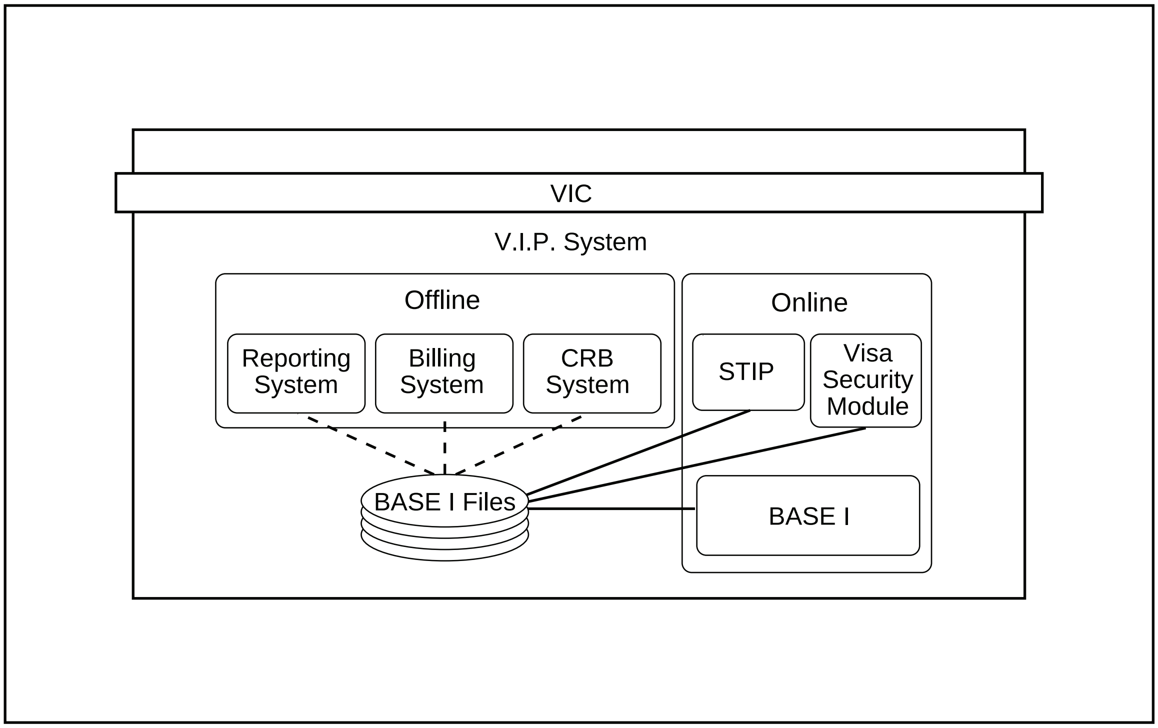
If Visa representatives cannot resolve a transaction failure issue at the regional level, they can contact Global Client Testing Support (IGSS) at itest@visa.com. IGSS provides first-level support coverage 24 hours a day, seven days a week, regarding transactional problems for BASE I, BASE II, SMS, and VSS, as well as for acceptance problems for international ATM and interregional POS locations. IGSS also provides testing with the VisaNet Certification Management Service (VCMS), the BASE II Service, and the Visa Test System VTS–V.I.P. tool. If IGSS is unable to resolve the issue, IGSS staff escalate problem tickets to the appropriate next level support group within Visa for resolution.

1.5 BASE I SYSTEM FUNCTIONS

BASE I provides online functions and offline functions. This section provides an overview of the basic functions that the BASE I System performs.

Figure 1-4 illustrates the BASE I software components and the system tables used for online and offline functions.

Figure 1-4 BASE I Software and Files

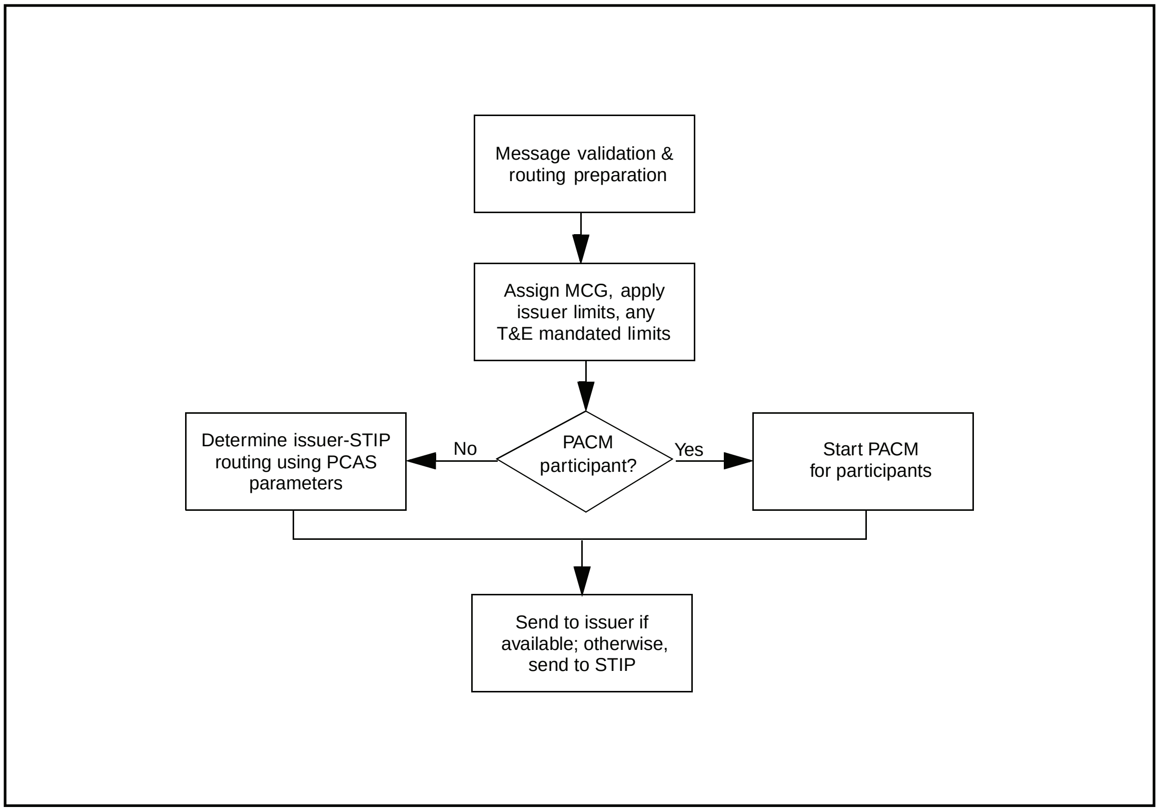


1.5.1 Online Functions

BASE I online functions comprise the processing of cardholder authorization requests and reversals and the generation of advices. As shown in Figure 1-5, online authorization functions include:

- Message validation and preparation.
- Message routing.
- Stand-in processing (STIP).

Figure 1-5 BASE I Message Preparation, Routing, and STIP


Message validation & routing preparation
Assign MCG, apply issuer limits, any T&E mandated limits
PACM participant?
No
Yes
Determine issuer-STIP routing using PCAS parameters
Start PACM for participants
Send to issuer if available; otherwise, send to STIP

Each VIC maintains a log of all requests and responses that the BASE I component processes. The system records key information in the message, not the entire message. BASE I passes the transaction information in the system log to the BASE I offline system components, which use the data for reporting, billing, and other administrative functions.

BASE I also supports online network management and administrative messages that control user access for BASE I processing and provide system status information to BASE I processing centers.

The following subsections describe the functions of BASE I online processing.

1.5.1.1 Message Validation and Preparation

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

BASE I also performs functions, or services, as specified by the member. These functions include:

- Message enhancement. (See Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for information about the Merchant Central File Service.)
- Visa Security Module (VSM) functions, including chip authentication, PIN translation, magnetic stripe or chip-based Card Verification Value (CVV or iCVV), Card Verification Value 2 (CVV2), Card Authentication Verification Value (CAVV), and Dynamic Card Verification Value (dCVV) verification.
- Currency conversion through the Multicurrency Service.
- Custom Payment Service (CPS) reimbursement program screening.

Refer to Chapter 3, Message Validation and Routing Preparation, for more information. Refer to *V.I.P. System Services, Volume 2*, for complete service information about the magnetic stripe- or chip-based Card Verification Value (CVV) Service, Card Verification Value 2 (CVV2) Service, CAVV Verification Service, PIN verification methods, PIN Verification Service (PVS), and the Multicurrency Service. For international CPS information, refer to the CPS ATM and CPS POS chapters in *V.I.P. System Services, Volume 2*. For U.S. CPS programs, refer to the latest edition of the *U.S. Interchange Reimbursement Fee Rate Qualification Guide*.

1.5.1.2 Message Routing

Message routing is an important function of BASE I. *Routing* refers to sending messages between VisaNet and acquirers and issuers. The term also applies to the decisions V.I.P. makes as to whether to route messages to issuers or to the stand-in processor (STIP).

NOTE

BASE I acquirers must use Visa-supplied account range routing tables for ATM transactions. BASE I acquirers can use, at their option, Visa-supplied account range routing tables for POS transactions. However, Visa requires acquirers in the U.S. region to use the POS Debit Device table.

BASE I first looks at several factors such as the account number, the source address, and the destination address when determining how to route a transaction.

BASE I 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 and when it is unavailable.
- Positive Cardholder Authorization Service (PCAS) parameters.
- Positive Authorization Capacity Management (PACM) Service parameters

Refer to Chapter 4, BASE I Limits and Routing, for more information about BASE I 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 BASE I routing decisions. For transactions with destinations outside of the VisaNet network, Gateway Services determine routing. Refer to *V.I.P. System Services, Volume 1*, for information about these routing services.

1.5.1.3 Stand-In Processing (STIP)

Stand-in processing (STIP) occurs when V.I.P. 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, BASE I uses issuer- or Visa-specified 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, decline, or refer a transaction include issuer-specified activity limits, advice limits, and any cardholder risk-level limits and random selection factors. Visa card issuers can maintain files of cardholder data at the VIC and can select the limits that control which transactions STIP can approve. Other card programs processed according to Visa rules are also eligible for STIP at the issuer's discretion.

Refer to Chapter 5, 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.

BASE I 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 BASE I advice file at their VIC.

Refer to *V.I.P. System Services, Volume 2*, for a complete description of advice recovery through the BASE I Advice Retrieval Service.

1.5.2 Offline Functions

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

- Reporting.
- Managing BASE I tables and databases.

For technical details about the BASE I offline functions described in this section, refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

1.5.2.1 Reporting

The BASE I reporting system generates various reports available to members by subscription. These reports describe BASE I 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.

BASE I 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
- Custom Payment Service (CPS) downgrade reports

Refer to *V.I.P. System Reports* for report information, including samples.

1.5.2.2 Managing BASE I Tables and Databases

BASE I 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), BASE I maintains records of routing and processing rules that apply to BINs, to processing centers, to stations, and, in the U.S. region and in

Visa Canada, to individual cardholder accounts. BASE I 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, BASE I can automatically update information in these BASE I databases at the time of the transaction.

V.I.P. also keeps records of the following relationships:

- Issuers to account numbers
- Issuers and acquirers to processing centers
- Processing centers to VICs
- Processing centers to network stations

Members must report any changes in account numbers and account ranges or in processing center designations to Visa. This information is vital to the correct routing of messages.

Cardholder Database Files

The *Cardholder Database* contains account numbers and other data that STIP uses to process address verifications, PIN verifications, preauthorized payments, 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 Global Client Testing Support (IGSS) at itest@visa.com. 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 1-1 lists the files contained in the Cardholder Database. Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, describes the files in more detail.

Table 1-1 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.
Address Verification File	This file contains cardholder billing address data. Issuers create and maintain this file.
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 POS. V.I.P. also uses it to create Cardholder Recovery Bulletins (CRBs).
PIN Verification File	Issuers create and maintain this file and the optional PIN Verification Service (PVS) 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.
Portfolio File	Issuers create and maintain this file and VisaNet uses it to decline or to return payment order requests from acquirers when V.I.P. finds a match. Refer to “Preauthorized Payment Cancellation Service (PPCS)” in this chapter.

Table 1-1 Cardholder Database Files (continued)

File	Summary Description
Risk-Level File	Issuers create and maintain this file and V.I.P. uses it for assigning and maintaining individual cardholder's risk levels, daily spending limits, and merchant group daily activity limits.

Merchant Central File

The *Merchant Central File* is a database created by and maintained by acquirers. The optional Merchant Central File Service (MCFS) uses the data in the Merchant Central File when acquirers want BASE I to insert more complete information into their authorization requests, for instance, when they cannot supply merchant category codes (MCCs). Merchant Central File information overrides what might be in the request when BASE I receives it. The file includes:

- Merchant names, cities, country codes, and category codes for Visa and MasterCard transactions.
- Terminal identifiers for American Express and Discover transactions.

Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for more information about the Merchant Central File.

1.6 SUMMARY OF BASE I PROCESSING SERVICES AND CAPABILITIES

BASE I processing support includes the following capabilities, services, and Visa card product family enhancements:

- Account-Level Programs and Cardholder Rewards
- Account or Address Verification-Only Status Checks
- Visa Advanced Authorization
- Auto-Substantiation Transactions
- Card Verification Value (CVV) Service, the Integrated Chip Card CVV (iCVV), and the Card Verification Value 2 (CVV2) Service
- Cardholder Authentication Verification Value (CAVV) Verification Service and Electronic Commerce Transactions
- Contactless Processing
- Credit Gateway Services, which support non-Visa transactions, such as those for MasterCard, Discover, Diners Club, American Express, and Japan Credit Bureau (JCB) International
- Custom Payment Service (CPS)
- Dynamic Card Verification Value (dCVV) Service
- Healthcare Eligibility Inquiries
- Incremental Authorization Processing
- Merchant Central File Service (MCFS)
- Merchant Verification Value (MVV) Processing
- Partial Amount Authorization
- Preauthorized Payment Cancellation Service (PPCS)
- Prepaid Authorization, Load, and Partial Authorization Processing
- Recurring Payment Processing
- Trusted Agent Program (TAP)
- U.S. Account Updater Verification (VAU) Service
- U.S. Bill Payment Processing

- Visa Cashback Processing: VisaNet Cashback Service
- Visa Commercial Card Large-Ticket Transactions
- Visa Personal Payments
- Visa POS Offers Redemption Platform (VPORP)
- Visa Product Eligibility Inquiries
- Visa Smart Debit/Smart Credit (VSDC)

1.6.1 Account-Level Programs and Cardholder Rewards

The *Visa Incentive Network (VIN)* allows Visa Canada and U.S. 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 BASE I 01*xx* dual-message or SMS 02*xx* 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—Product ID. V.I.P. adds this field to authorization or financial requests to identify the specific card product for the issuer. V.I.P. retrieves the values from the Cardholder Database (CDB) according to the specific cardholder. Issuers update the CDB with the Cardholder Maintenance File. Refer to the pertinent V.I.P. technical specifications manuals for more information.

1.6.2 Account or Address Verification-Only Status Checks

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).
- Field 52—PIN Data, and Field 53—Security-Related Control Information are present, or Field 123—Verification Data is present, or 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.

1.6.3 Visa Advanced Authorization

Visa Advanced Authorization provides transaction risk assessment to issuers for Visa card cardholders during the POS and ATM authorization request process. Visa Advanced Authorization is required for U.S. issuers and is a subscription-based service for issuers in Visa Canada and the Asia-Pacific (AP), Latin America and Caribbean (LAC), and Central and Eastern Europe, Middle East, and Africa (CEMEA) regions. To receive the Visa Advanced Authorization fields, Field 62.21—Advanced Authorization Risk Score and Field 62.22—Advanced Authorization Condition Code, in an authorization request, the issuer must first perform testing. STIP does not include the Advanced Authorization risk scoring results in its approval or decline decision.

1.6.4 Auto-Substantiation Transactions

Available in the U.S. region only, cardholders make *auto-substantiation transactions* for purchases eligible for Flexible Spending Accounts (FSAs) or Healthcare Reimbursement Arrangements (HRAs) as defined by Internal Revenue Service (IRS) regulations. These transactions allow employers and their third-party service providers to approve over-the-counter (OTC) qualified medical expenses from participating retailers at the time of purchase. This capability reduces the need for consumers to make a purchase and later have to submit sales receipts for employer reimbursement. In addition to supporting partial authorizations, auto-substantiation transactions are valid for FSA card-based transportation purchases such as commuter tickets, parking passes, and mass transit vouchers and tickets.

V.I.P. force-routes auto-substantiation transactions to issuers for approval or decline decisions. The issuer forwards the request to the cardholder’s health insurer; the insurer returns the result—approval for the full or partial amount, or decline altogether.

Positive Authorization Capacity Management (PACM) Service processing does not apply to auto-substantiation transactions. V.I.P. passes the message to available issuers without performing any service-specific editing; STIP declines unavailable-issuer requests with response code **91** (issuer unavailable) in Field 39—Response Code. If the issuer is unavailable for reversals, STIP responds with response Code **21** (no action taken in field 39).

The key fields in original 0100 and 0200 auto-substantiation requests are:

- Field 54—Additional Amounts: Positions 3–4 contain the amount type. Valid values are:
  - Code **4T**—Amount Transit (not applicable to healthcare auto-substantiation transactions)
  - Code **4S**—Total Amount Healthcare (for over-the-counter [OTC] amounts only, or for the grand total of any one or more of the following health-related amounts plus any OTC amount, if applicable)
  - Code **4U**—Amount Prescription/Rx
  - Code **4V**—Amount Vision/Optical
  - Code **4W**—Amount Clinic/Other Qualified Medical
  - Code **4X**—Amount Dental

NOTE

Field 54 also appears in 0400 and 0420 reversals. This usage of field 54 is not present in original responses, reversal responses, advice responses, or any related exception transactions. This usage of field 54 appears in 0120, 0220, and 0420 STIP advices when it is present in the original request or reversal.

Acquirers must include this field in 0100 and 0200 healthcare auto-substantiation requests. If V.I.P. receives an 0100, 0200, 0400, or 0420 message that contains this usage of field 54 and field 62.20 does not include a valid MVV for a SIGIS-certified merchant, V.I.P. retains all field 54 amount sets from the request message and resets the value in field 62.4 to a new Market-Specific Data Identifier (MSDI) indicating that the merchant has not successfully completed testing for IIAS processing.

V.I.P. does not require a field 54 set with healthcare information for healthcare auto-substantiation 0400 and 0420 reversal messages, but if it is present, the acquirer should also include field 62.4 and field 62.20.

- Field 60.10—Partial Authorization Indicator: This field must contain **1** (acquirer supports partial authorizations).
- Field 62.20—Merchant Verification Value: Acquirers must include a valid MVV for a SIGIS-certified merchant in 0100 and 0120, and 0200 and 0220 request messages they send to VisaNet. Otherwise, V.I.P. drops the healthcare data from the message.
- Field 62.4—Market-Specific Data Identifier: This field must contain **M** (medical; healthcare) in over-the-counter (OTC) 0100 and 0200 requests, 0400 and 0420 reversals, and related advices, or **T** (transit; in healthcare transactions only) in 0100 and 0200 requests, 0400 and 0420 reversals, and related advices. In original requests, the value must be consistent with a corresponding value of **4S** (healthcare) or **4T** (transit) in field 54. Issuers should include the field in responses, but if it is missing, V.I.P. reinstates it.

  When any of the following conditions apply, V.I.P. replaces the **M** or **T** in field 62.4 with **N** in the request message to the issuer:
  - The original request does not include a value of **4S** or **4T** in field 54.
  - The issuer does not accept field 54 in request messages.
  - The original request includes field 54 with the value **M** but does not include field 62.20.

  When the merchant is not SIGIS-certified, V.I.P. includes a new MSDI in field 62.4 in the response to the acquirer to indicate that the merchant has not successfully completed testing for IIAS processing. The acquirer must include the value received in the response in the clearing and settlement transaction and any subsequent exception transactions. The acquirer may include this field in reversals, but V.I.P. stores the value from the original transaction and includes it in the reversal request to the issuer and also in the response back to the acquirer.

  For Custom Payment Service (CPS) submissions that qualify, V.I.P. uses the code in field 62.4 when calculating the validation code in field 62.3.

IMPORTANT

Issuers must include field 62.4 in 0110 auto-substantiation responses for both Visa and MasterCard transactions.

V.I.P. and issuer processing depends on whether the amount in field 4 equals the amount in field 54, positions 9–20; or the amount in field 4 is greater than the amount in field 54, which means the transaction is a partial authorization.

In the event of an IRS audit, the issuer asks the merchant for details of healthcare product line items on specific transactions. The request contains the issuer's fax number for merchants to use to send the healthcare receipt data.

1.6.5 Card Verification Value (CVV) Service, the Integrated Chip Card Card Verification Value (iCVV), and the Card Verification Value 2 (CVV2) Service

Issuers can choose to have the BASE I Visa Security Module (VSM) verify the following verification values all of the time or only when the issuer is unavailable and STIP processes the transaction.

- A *card verification value (CVV)* is a 3-digit number encoded on the card's physical magnetic stripe or in the chip's image on a Visa Smart Debit/Smart Credit (VSDC) card.
- An *Integrated Chip Card card verification value (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*. A VSDC card's chip image may contain either the CVV or the iCVV. An iCVV is not used on a card's physical magnetic stripe.
- The *Card Verification Value 2 (CVV2)* is an embossed 3-digit security number appearing on the reverse side of the card. It can be used in both card-present and card-not-present transactions.

Visa offers a verification service for the following:

- Card Verification Value (CVV or iCVV) for card-present transactions.
- Card Verification Value 2 (CVV2) for card-present and card-not-present transactions.

NOTE

The CPS/Account Funding program requirements include the CVV2 for electronic commerce (e-commerce) stored-value transactions. For stored-value cards that are to be refilled more than once, the program requires the CVV2 only in the initial funding request for the request to qualify; subsequent transactions can qualify for the CPS program without the CVV2 being present.

1.6.5.1 CVV and iCVV

Determining whether V.I.P. 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, V.I.P. performs CVV processing only if the CVV is in the correct position in the track. Refer to the *Payment Technology Standards Manual* for technical specifications for CVV placement.

- If field 22, positions 1 and 2, contain **90** or **05** and the issuer's system settings indicate that V.I.P. 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 and Interlink 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**, V.I.P. assumes that the track data originated from the chip. V.I.P. checks the issuer's system settings (in CORE) to determine if the verification value in the track data is a CVV or an iCVV (Set A indicates CVV, Set B indicates 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 code **90** in field 22 does not guarantee CVV processing. If a non-participating acquirer submits code **90** in field 22, V.I.P. rejects the message.*

  Validation of the CVV or the iCVV residing in the chip's magnetic stripe image 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, V.I.P. (or the issuer) uses the DES 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.

As indicated above, iCVV processing uses all options, parameters, and keys used in CVV processing. V.I.P. 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 expiration 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 V.I.P. can approve, refer, or decline transactions that fail CVV validation depending on issuer-specified parameters.

Refer to the Card Verification Value (CVV) Service chapter in *V.I.P. System Services, Volume 2*, for a description of the service. Refer to the *Payment Technology Standards Manual* for technical specifications for CVV placement, calculation, and verification.

1.6.5.2 Card Verification Value 2 (CVV2)

Members use Card Verification Value 2 (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 expiration date to recalculate a CVV2, which V.I.P. 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 V.I.P. validate the CVV2 for them, or can do both. If V.I.P. performs the validation, it verifies the CVV2 before it passes the authorization request to the issuer or to STIP. Issuers can choose to have V.I.P. check the CVV2 in all CVV2-eligible authorization requests.

Depending on regional requirements and on issuer participation, V.I.P. 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; V.I.P. 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.

V.I.P. 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.

Refer to the Card Verification Value 2 (CVV2) Service chapter in *V.I.P. System Services, Volume 2*, for a description of this service.

1.6.6 Cardholder Authentication Verification Value (CAVV) Verification Service and Electronic Commerce Transactions

The *Cardholder Authentication Verification Value (CAVV) Verification Service* is a risk control service used to authenticate the cardholder in electronic commerce (e-commerce) authorization transactions. The process involves two phases:

1. Verified by Visa (VbV)
2. CAVV Verification Service

During the VbV phase, the cardholder is electronically identified and a CAVV is generated that is associated with the purchase.

The CAVV Verification 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 VbV phase in the request. When the CAVV is present in the transaction, the issuer or V.I.P. verifies that the CAVV in the message matches the CAVV generated during the VbV phase. If V.I.P. or the issuer verifies the CAVV, the transaction is protected from certain chargebacks should disputes arise later.

When the issuer or V.I.P. (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 V.I.P. on behalf of the issuer, uses Data Encryption Standard (DES) 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 V.I.P. perform verification on their behalf must provide Visa with their DES keys.

Visa offers two classifications of CAVV Verification Service processing options to issuers that participate in VbV: Authentication or Attempt. Visa 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 classifies a transaction as an *Authentication* when the acquirer, the issuer, and the cardholder all participate in VbV.

Attempt—With this option, the issuer or V.I.P. generates a CAVV for attempted transactions. Visa classifies a transaction submitted by a participating acquirer as an *Attempt* when either the issuer or the cardholder does not participate in VbV. Liability shifts for these types of transactions. This option is mandatory in some regions.

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:

- Standard Issuer CAVV Service/Standard Decline/Failure option, with which V.I.P. 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 Verification Results to the Issuer option, with which VisaNet performs all validations on the issuer's behalf, and forwards all status results of transactions to the issuer.
- Issuer Supports Own CAVV Verification option, with which VisaNet forwards the transactions to the issuer to perform validation. The issuer returns the status results in the response messages.

Depending on the region, VisaNet assesses interchange reimbursement fees (IRFs) based on the CAVV Verification Service classification of the e-commerce transaction.

The CAVV Verification Service supports both magnetic stripe Visa cards and Visa Smart Debit/Smart Credit (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, Visa Corporate, or Visa Purchasing cards. When V.I.P. validates a CAVV in an ineligible transaction, V.I.P. generates code **B** in field 44.13. Only V.I.P. is allowed to generate this 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 account into a single, larger transaction and submit it for payment processing. Aggregation reduces acquirers' interchange fees. 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, V.I.P. changes the value in field 62.4 from **E** to **N**. V.I.P. 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 VbV and CAVV as well as about the CAVV Verification Service key fields, refer to *V.I.P. System Services, Volume 1 and Volume 2*, and to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

1.6.7 Contactless Processing

Cardholders make *contactless transactions* using contactless chip Visa cards. A Dynamic Card Verification Value (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 Visa Smart Debit/Smart Credit (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.

V.I.P. 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 U.S.A. (U.S.) 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

V.I.P. supports chip cards having an alternative primary account number (PAN) stored on the chip. This PAN is different from the PAN embossed on the card and serves as a security measure to prevent counterfeit chip cards from being used for non-chip transactions. Alternative PAN processing supports contactless chip cards using qVSDC, VSDC, and magnetic-stripe data. V.I.P. account ranges can be set up to indicate alternative PAN support. V.I.P. declines a transaction with response code **59** (suspected fraud) if all of the following apply:

- The account range of the card indicates that it supports an alternative PAN.
- Field 22 does not contain **05**, **07**, **91**, or **95**.
- Chip data is not present in field 55 or the third bitmap fields.

Visa payWave ATM Transactions—V.I.P supports Visa payWave ATM transactions in network 0002 and network 0004. Acquirers that choose to implement Visa payWave ATM transactions must support full chip data.

Acquirers that implement these transactions for the first time must use full chip data in Field 55, Usage 1—VSDC Chip Data. However, acquirers that currently use the expanded third bitmap format may continue to use their existing format for processing Visa payWave ATM transactions.

1.6.8 Custom Payment Service (CPS)

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. V.I.P. matches a transaction's clearing and authorization messages using a unique transaction identifier (TID) assigned by V.I.P. before it forwards requests to issuers or to STIP. CPS processing applies to Visa card POS transactions, to international Visa 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 is specific fee edit criteria for each CPS program.

CPS requires acquirers to include Field 62.1—Authorization Characteristics Indicator to signal to BASE I 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. The V.I.P. System assigns a TID in field 62.2 to all transactions before BASE I forwards the request to the issuer or to STIP. Refer to "Merchant Verification Value (MVV) Processing" in this chapter.

V.I.P. uses the values in Field 60.1—Terminal Type and Field 60.2—Terminal Entry Capability to determine specific transaction types.

BASE I accepts certain CPS transactions either in fixed format or in bitmap format. Bitmap format is required for participation in the full range of CPS markets; fixed format is not valid for incremental authorizations, for recurring payments, for mail order, telephone order, and electronic commerce (MOTO/EC) transactions, or for partial reversals.

For international CPS information, refer to the CPS ATM and CPS POS chapters in *V.I.P. System Services, Volume 2*. For U.S. CPS programs, refer to the latest edition of the *U.S. Interchange Reimbursement Fee Rate Qualification Guide*.

1.6.9 Healthcare Eligibility Inquiries

Visa *healthcare eligibility inquiries* allow healthcare providers to determine whether a cardholder's health insurance coverage is current. These U.S. region-only 0100 authorization requests and 0110 responses are non-financial, information-only transactions. Eligibility inquiries are valid for BASE I, SMS POS, and Interlink.

The key eligibility inquiry fields in 0100 authorization request are:

- Field 3—Processing Code: Positions 1–2, must contain **39** to indicate an eligibility inquiry.
- Field 4—Amount, Transaction: The field must contain **zero**. If the acquirer sends a different amount, V.I.P. changes it to **zero**.
- Field 104—Transaction-Specific Data: This field contains one or more specific TLV-formatted datasets that include the healthcare provider's ID and HIPAA healthcare treatment code if applicable. V.I.P. forwards the field to issuers that have successfully completed testing; otherwise it drops it. Refer to "Field 104—Transaction-Specific Data" in the BASE I or SMS technical specifications manuals for further information.

0110 responses include the following key fields:

- Field 54—Additional Amounts: This field contains the co-payment amount in the following format:
  - Positions 1–2, Account Type contain **00**
  - Positions 3–4, Amount Type contain **3S**
  - Positions 5–7, Currency Code contain **840** for U.S. dollars
  - Position 8, Amount, Sign contains **C** for positive balance
  - Positions 9–20, Amount contain the cardholder's co-payment amount.

NOTE

*If field 54, positions 1 and 2, and field 3.2 contain **00** or **40**, V.I.P. changes the value in field 54, positions 1 and 2, to match the value in field 3.2.*

- Field 4—Amount, Transaction: The field must contain **zero**. If the acquirer sends a different amount, V.I.P. changes it to **zero**.
- Field 104—Transaction-Specific Data: In responses, in addition to the field 104 data from the request, the field includes data that applies to the approval or decline decision, such as health insurance carrier, payer ID, or approval or reject reason codes. Refer to the Field 104—Transaction-Specific Data section of the BASE I or SMS technical specifications manuals for further information.

Visa U.S.A. members must successfully complete testing that they can support the field 3 processing code (**39**) and the field 54 amount type (**3S**). Participation is limited. Interested members can contact their Visa representatives for further details.

1.6.10 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.

Endpoints must not decline incremental authorizations by treating them as duplicate transactions. In incremental authorization requests and their reversals, the field 11 and field 37 values match the corresponding values in the original authorization request message, and the field 62.2 value matches the corresponding value in the original authorization response message.

1.6.11 MasterCard Processing Through VisaNet

Credit POS Processing—Gateway Services route POS MasterCard transactions from Visa acquirers to MasterCard issuers, automatically converting the VisaNet-format messages to MasterCard's Banknet format. Similarly, Gateway Services automatically convert Banknet-format responses from issuers to the VisaNet format for delivery to Visa acquirers.

ATM Processing—BASE I does not send PIN-based ATM MasterCard transactions to Banknet; V.I.P. declines them with response code **81** (cryptographic error found) in field 39. VisaNet supports PIN-based cash disbursement transactions if the issuer can receive them directly through VisaNet as 0200 full financial messages destined for Plus or CIRRUS SMS issuer BINs.

MasterCard transactions or transaction elements supported by Visa include the following:

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 *Credit Gateway Service (CGS) Cross-Reference Guide* describes these transactions and elements. The gateway also sends VisaNet-acquired Diners Club authorization requests with Diners Club or MasterCard account numbers to the Discover network; VisaNet no longer routes Diners Club requests to Diners Club.

For details about how the gateway function transfers data between networks, refer to the *Credit Gateway Service Cross-Reference Guide*. This document includes field-by-field data transfer descriptions between VisaNet-format dual-message 0100 authorization requests and 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.

For Visa issuers that process MasterCard purchase or cash transactions using the Visa Shortest Online Path (VSOP) Service, BASE I determines issuer availability. V.I.P. routes transactions to available issuers; if issuers are unavailable, V.I.P. routes transactions to Banknet. If Banknet or the issuer fails to respond, V.I.P. declines the transaction. VisaNet does not provide stand-in processing for MasterCard transactions. The VSOP Service is available to MasterCard-issuing Visa issuers outside of the U.S. region. Refer to the VSOP Service chapter in *V.I.P. System Services, Volume 1*, for further information and processing requirements.

1.6.11.1 MasterCard 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—VisaNet does not convert amounts to U.S. dollars. For requests, the Visa Gateway transfers the VisaNet field 4 amount to Banknet DE 4 while retaining the acquirer's local currency, and it transfers the currency code from VisaNet field 49 to Banknet DE 49 without changing the acquirer's original code.

V.I.P. 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 U.S. dollars and V.I.P. changes the currency code in field 49 and DE 49 to **840**. Additionally, V.I.P. also changes the currencies in 0100 MasterCard authorization requests sent by Visa SMS acquirers to Banknet to U.S. dollars, regardless of the currency type originally assigned.

The only editing V.I.P. performs is to ensure the field 49 currency code in the request message is valid. V.I.P. rejects the message if the currency code is invalid.

Participation in this MasterCard multicurrency feature is optional, but both the PCR and acquiring BIN must participate.

1.6.11.2 Processing Domestic MasterCard Transactions in Malaysia

In Malaysia, Visa members can process certain VisaNet-acquired *domestic* (the merchant, the acquirer, and the issuer are all in the same country) MasterCard transactions entirely within VisaNet and do not have to send them to Banknet. VisaNet processes all transactions in V.I.P. format.

Credit POS Processing—Eligible transactions are PIN- and non-PIN-based POS transactions. MasterCard issuers must be Visa members and be connected directly to VisaNet so they can receive their MasterCard transactions through VisaNet. Also available to participating members are the Card Verification Value (CVV) Service, the Card Verification Value 2 (CVV2) Service, and the Positive Cardholder Authorization Service (PCAS).

The Visa CVV and CVV2 services are similar to MasterCard's CVC and CVC2 services, respectively. Both Visa and MasterCard use the same CVV and CVV2 algorithms.

Debit and ATM Processing—The PIN Verification Service (PVS) supports MasterCard PIN verification. Participating issuers must supply Visa with their encryption keys if they want V.I.P. to perform these services. In request messages, Field 32—Acquiring Institution Identification Code must contain the acquirer's Visa BIN that signed the MasterCard-accepting merchant that participates in the service. For PIN-based requests, field 32 must contain the code for the acquirer associated with the Acquirer Working Key (AWK) used to encrypt the PIN. For participating issuers, VisaNet sends non-domestic PIN-based transactions to Banknet if issuers are unavailable.

1.6.12 Merchant Central File Service (MCFS)

Through the *Merchant Central File Service (MCFS)*, BASE I and SMS can enhance the message content with POS terminal information that the merchant or the acquirer is unable to supply. Depending on the card type, record format, and acquirer specifications, BASE I and SMS can augment the following fields in the Merchant Central File:

- Merchant category code (Field 18—Merchant Type)
- Terminal identification (Field 41—Card Acceptor Terminal Identification)
- Card acceptor name and location (Field 43—Card Acceptor Name/Location)
- ZIP or postal code (Field 59—National Point-of-Service Geographic Data)
- Merchant verification value (Field 62.20—Merchant Verification Value [MVV])
- Vendor identification (check acceptance) (Field 100—Receiving Institution Identification Code)

Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, and to the Cardholder Database chapter in *V.I.P. System SMS Processing Specifications (U.S.)*, for more Merchant Central File information.

1.6.13 Merchant Verification Value (MVV) Processing

V.I.P. 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 assigns the first six positions and helps the acquirer assign the last four; if the field format is invalid in requests, V.I.P. drops the field. Acquirers and issuers must successfully complete testing to receive this field. The MVV is not necessarily a component of the Custom Payment Service.

1.6.14 Partial Approval Authorizations

VisaNet supports partial amount authorizations involving multicurrency processing for prepaid cards processed as BASE I dual-message and SMS single-message transactions for all regions. Responses can include account balances along with the partial approval 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 approvals.

NOTE

Acquirers can include partial authorization requests in status check transactions. The issuer may respond with an amount in field 4 that is the maximum authorized amount for the purchase. These responses also contain response code ***10*** *in field 39.*

1.6.14.1 Key Fields and Rules for Partial Approvals With Multicurrency Processing

The following table lists partial approval key fields for 0110 and 0210 responses.

Table 1-2 Key Fields for Partial Approval 0110 and 0210 Responses

Field	Description
Field 4—Transaction Amount	Contains the partially approved amount from the issuer.
Field 6—Cardholder Billing Amount	Contains the amount in field 4 in the cardholder billing currency if multicurrency processing is involved in the transaction.
Field 39—Response Code	Contains code **10** for partial approvals.

Table 1-2 Key Fields for Partial Approval 0110 and 0210 Responses (continued)

Field	Description
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. 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: 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). Positions 3–4—Amount Type: These positions contain code **57** (for original amount). Positions 5–7—Currency Code: These positions contain a 3-digit code that identifies the amount in positions 9–20. Position 8—Amount Sign: This positions contains code **C** (positive balance) or **D** (negative balance) 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).*

V.I.P. returns the issuer's response with reject code **0150** if field 39 contains code **10**, but field 54 contains any of the following errors:

- The field is missing.
- The partial approval 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 code **10**, V.I.P. 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, V.I.P. returns the transaction to the issuer with response code **0736**.

If the original transaction amount is not present in field 54 for a partial approval, V.I.P. inserts the original amount in field 54 before forwarding the 0110 response to the acquirer.

V.I.P. sends rejected transactions to 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.

1.6.14.2 Partial Approvals With No Multicurrency Processing Rules

If the 0110 or 0210 response contains code **10** in field 39, and field 4 is missing, V.I.P. 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, V.I.P. 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 approval transaction, V.I.P. inserts the original amount in field 54 before forwarding the response to the acquirer.

NOTE

V.I.P. 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 approved authorizations, 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).

1.6.14.3 Processing Balances With Multicurrency Processing and Optional Issuer Fees

For field 54 sets that contain balance information in cross-border transactions, if the cardholder billing currency is not the same as the transaction currency, V.I.P. replaces the balance amount in the cardholder 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 approval prepaid card transactions 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 cardholder 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. V.I.P. does not deduct the OIF from the balance amount when it converts the balance from the cardholder billing currency to the transaction currency.

1.6.15 Preauthorized Payment Cancellation Service (PPCS)

The *Preauthorized Payment Cancellation Service (PPCS)* enables issuers to stop payments on preauthorized payment transactions, such as those for recurring or installment payments.

Participating issuers place stop-payment orders in the Portfolio File in the Cardholder Database (CDB). When acquirers submit a preauthorized payment transaction, V.I.P. checks the database and if it encounters a stop payment order for that account number, it declines the request.

PPCS enables members to meet Federal Reserve *Regulation E* requirements, which govern electronic funds transfers and provide U.S. cardholders with certain dispute rights for check card transactions. Members that issue check cards must comply with the terms of those regulations.

PPCS is available both to BASE I users and to SMS users. PPCS is optional for issuers, and is established at the BIN level.

PPCS is not an acquirer service, and acquirers and merchants have no ability to determine whether their transactions are checked by PPCS. If a merchant deals in preauthorized-type transactions, then any one of those transactions is potentially eligible for PPCS checking on behalf of participating issuers. Acquirer participation in PPCS is mandatory to the extent that they must be able to receive PPCS response codes. Acquirers must modify their systems to recognize the PPCS decline response codes **R0**, **R1**, and **R3** in 0110 authorization and 0210 financial response messages.

Participating issuers place stop payment instructions from their cardholders in the Portfolio File in the Cardholder Database (CDB) using 0302 file maintenance request messages or using Visa Resolve Online (VROL). In 0302 messages, issuers place an action code in Field 91—File Update Code to indicate the action V.I.P. is to take with the file record: add, delete, replace, or inquire.

V.I.P. checks the Portfolio File in the CDB when it receives an 0100 or 0200 automatic payment request from an acquirer or a merchant and uses the results to determine authorization decisions. VisaNet supports the following types of cardholder-initiated stop-payment commands:

- **R0**—Stop Payment Order
- **R1**—Revocation of Authorization Order
- **R3**—Revocation of All Authorizations Order
- **C2**—Revocation of All Authorizations Order

NOTE

*The **C2** stop payment code is used* only *by BASE II users.*

If V.I.P. encounters no stop-payment code, it continues normal request processing.

If V.I.P. encounters a stop-payment code, V.I.P. routes the request to STIP. STIP declines the request using the stop-payment code from the Portfolio File record (**RO**, **R1**, or **R3**) as the response code in field 39. The STIP action is indicated by a value of **4** in Field 44.1—Response Source/Reason Code in responses and in issuer advices.

V.I.P. checks on issuer participation to prevent issuers that are not properly configured for PPCS from adding PPCS records to the CDB. If the issuer sending in an 0302 maintenance transaction with code **PF** in field 101 and code **1** (add), **3** (delete), **4** (replace), or **5** (inquiry) in field 91, V.I.P. checks CORE to see if the issuer is a participant. If not, V.I.P. declines the transaction with code **06** (error) in field 39 and inserts error code **0684** (BIN does not participate in service) in field 48, usage 1B.

(Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for further information about the Portfolio File in the CDB. Refer to *V.I.P. System Services, Volume 2*, for the PPCS service description.)

1.6.16 Prepaid Activation, Load, and Partial Approval Processing

V.I.P. processes prepaid cards for Visa and private-label card products, as well as for Interlink. Merchants and issuers submit transactions to activate new prepaid cards and to load spending amounts onto activated cards.

In the U.S. and Canada regions, the Visa ReadyLink Service activates and loads Visa prepaid cards through VisaNet. V.I.P. identifies Visa ReadyLink Service participants by checking the Visa Routing file, the Consolidated Routing file, and the PIN at Point of Sale routing file. Each of these files contains a Visa ReadyLink Participant Indicator. A value of **Y** in the indicator signifies that the card range participates in the Visa ReadyLink Service.

The ReadyLink Service supports electronic fare load transactions, which enable chip cards to be used for contactless access to a transit system. U.S. acquirers that choose to support these transactions must be able to send the access token account number for the cardholder's chip card in field 102. U.S. issuers that choose to support these transactions must be able to receive field 102.

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 V.I.P. 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. Refer to “Partial Approval Authorizations” in this chapter for partial approval processing 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 successfully completed testing that they can send and receive prepaid transactions.

1.6.17 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 card-present (face-to-face POS) or card-not-present (MOTO or e-commerce) environments. Merchants automatically initiate subsequent, or recurring, transactions without the cardholder being notified beforehand or necessarily being present.

The presence either of **02** in Field 60.8—Mail/Phone/Electronic Commerce and Payment Indicator, positions 9–10, or 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 U.S. region and is optional for non-U.S.-acquired transactions. A value of **R** in field 126.13 is required for recurring payment transactions originating from an acquirer outside of the U.S. region and is optional for U.S.-acquired transactions. Depending on the region, acquirers may send both fields with their recurring payment codes in the same request.

Both fields (field 126.13 and field 60.8) and their values are valid for chargeback protection. If the issuer has not successfully completed testing to receive field 126.13, V.I.P. drops it before forwarding the request to the issuer and inserts code **02** in field 60.8.

VisaNet force-routes recurring payment requests to issuers, bypassing PACM processing. 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 expiration dates have expired or are missing. Issuers can choose, however, to have STIP approve these transactions according to issuer-specified parameters.

1.6.18 Trusted Agent Program (TAP)

The *Trusted Agent Program (TAP)*, formerly called the Visa Agent Identification Service (AIS), informs acquirers in the U.S. region of merchants that are using unregistered agents (including third-party servicers and merchant servicers) to submit transactions to VisaNet using the acquirer's BINs. Unauthorized VisaNet access compromises the security of the Visa payment system and exposes Visa members to considerable risk from theft and fraud. Although acquirers are financially liable for all transactions submitted under their BINs, they are often unaware of the merchant-agent arrangements because the transactions pass through agents to VisaNet, bypassing the acquirer.

TAP greatly reduces acquirers' risk by monitoring transactions submitted through acquiring agents to VisaNet and then reporting unauthorized use of BINs to acquirers. Tap identifies unregistered agents and logs them for acquirer registration and Visa risk analysis.
TAP applies to all 0100 and 0200 authorization and full financial request messages processed through BASE I, SMS POS, and SMS Interlink.

Visa assigns each agent a secret code and unique ID. When an agent receives a request from a merchant, the agent constructs the contents of Field 126—Agent Unique Account Result (AUAR), by hashing the secret code, unique ID, and the account number according to a Visa-specified algorithm. The agent forwards the AUAR to the acquiring VisaNet processor along with the other merchant information for submission to VisaNet.

If an acquiring processor receives the merchant's authorization request or full financial request message from the agent but the agent did not include the AUAR, the acquiring processor uses a Visa-supplied default AUAR for the VisaNet submission. If an acquiring processor receives requests directly from a merchant, field 126.18 is not required and must not be present in the request.

V.I.P. does not edit the field; it also does not send it to the issuer processor nor does it return field 126.18 in the response. VisaNet validates the field offline and sends summary reports to the acquirers or to their designates.

Currently, U.S. acquirers and their processors can optionally support TAP. They can test now to send field 126.18. Visa will require all U.S. acquirer processors to support TAP at a later date.

1.6.19 U.S. Account Updater Verification (VAU) Service

The *Account Updater Verification (VAU) Service* enables both BASE I and SMS acquirers and V.I.P. to query cardholders' accounts in the Global Customer Assistance Service (GCAS) databases. VAU is an optional service that enables the secure electronic transmission of updated account information among participating issuers, acquirers, and merchants that process Visa transactions using account information they keep on file.

The service also enables acquirers to update the databases with current information. Participating acquirers use 0100 authorization messages that include the:

- Replacement account number
- Replacement expiration date
- Account status codes
- Credit limit information
- Card product type code
- Type of card

Participation in the service requires testing. Acquirers, issuers, and merchants that choose to participate in the Account Updater Verification Service can contact their Visa representatives.

1.6.20 U.S. Bill Payment Processing

U.S. bill payment transactions are a type of Visa non-T&E POS purchase transaction supported only in the United States (U.S.) region and in U.S. territories when initiated by U.S. merchants. VisaNet supports U.S. bill payment transactions for all PDG networks. Bill payment transactions can be initiated online, by mail, or in person. Bill payment transactions are eligible for Custom Payment Service (CPS) processing.

> **NOTE**
>
> *U.S. territories in which VisaNet supports bill payments are American Samoa, Guam, Northern Marianas Islands, Palau, Puerto Rico, American Virgin Islands, U.S. Minor Outlying Islands, and Marshall Islands.*

V.I.P. treats bill payment transactions as regular POS transactions, for instance, it applies most of the edits, processes, and routing parameters appropriate for the actual type of bill payment transaction (card-not-present, e-commerce, and other transactions). However, bill payment transactions cannot be PIN-based and they are ineligible for Positive Authorization Capacity Management (PACM) Service, or Priority Routing Service. Bill payment transactions without PINs are eligible for the PIN Debit Gateway Service (PDGS).

V.I.P. declines non-POS transactions, non-U.S.-acquired transactions, and transactions from non-U.S. merchants (excluding those in U.S. territories) with result code **12** (invalid transaction) in Field 39—Response Code.

Key fields for bill payment transactions are:

- Field 3—Processing Code: This field must contain **50**. V.I.P. downgrades the transaction according to CPS rules if the code in field 3 is not **50**. V.I.P. supports processing code **50** in all original authorization and financial transactions, and their reversals, as well as exceptions (chargeback and representments). Preauthorizations and their completions, adjustments, fee collections and funds disbursements, collection-only transactions, and fraud messages do not use code **50**.
- Field 25—POS Condition Code: The code in this field must be appropriate for the manner in which the transaction was submitted. Refer to the pertinent BASE I or SMS POS technical specifications manuals for the valid POS condition codes. Note that mail order and telephone order (MOTO) indicators are not limited to MOTO bill payment transactions; for instance, field 25 can contain **00** for a card-present recurring bill payment transaction.
- Field 62.1—ACI: The code in this field must be **Y**; otherwise, V.I.P. downgrades the transaction.
- Field 62.4—Market-Specific Data Identifier: The identifier in this field must be **B**. If the value is not **B**, or the field is not populated, V.I.P. rejects the transaction with Reject Code **0626**—Invalid Value for Bill Payment Transaction, or Reject Code **0492**—Value Missing for Bill Payment Transaction. Only bill payment transactions use the identifier **B.**

Bill payment type indicators are different for BASE I and for SMS. The type indicator for BASE I is in Field 60.8—Mail/Phone/Electronic Commerce and Payment Indicator. For SMS, it is located in Field 63.6—Chargeback Reduction/BASE II Codes. There are four types of bill payment transactions. The following table lists the types and their field codes.

Table 1-3 Bill Payment Transaction Types and Field Codes

Type of Bill Payment	Field Code
Manual Payment—Single, one-time payment initiated by the cardholder.	**01**
Recurring Payment—Multiple, ongoing payments for an indefinite term, until the cardholder or biller cancels the recurring payment arrangement.	**02**
Installment Payment—Multiple payments for a specified term, usually until payment has been satisfied.	**03**
Electronic Commerce Payments—	
Secure e-commerce payment	**05**
Non-authenticated security transaction from 3-D Secure-capable merchant that attempted to authenticate using 3-D Secure.	**06**
Non-authenticated security transaction.	**07**
Non-Secure Transaction.	**08**

For CPS card-not-present submissions, V.I.P. does not require address data for acquirers to receive an authorization characteristics indicator (ACI) of **V**—meets address verification requirements. Field 62.4—Market-Specific Data Identifier is optional in 0110 and 0210 responses from issuers. If necessary, V.I.P. inserts it in the response to the issuer.

If a bill payment transaction is destined for a non-U.S. issuer, V.I.P. logs the message as a bill payment, replaces the field 3 processing code **50** with **00**, and drops field 62.4. When V.I.P. receives the response from the issuer, it restores processing code **50** and inserts field 62.4 before forwarding the message to the acquirer.

1.6.21 Visa Cashback Processing: VisaNet Cashback Service

The *VisaNet Cashback Service* provides domestic cashback transaction capability for participating regions. A domestic cashback transaction indicates that the merchant, acquirer, and the issuer reside in the same country. Regions can choose to implement cashback processing capability as either a domestic-specific solution without VisaNet, or they can participate in the VisaNet Cashback Service.

Cashback processing is optional for issuers, for acquirers, and for merchants in all Visa regions. Participating regions and countries within those regions establish maximum cashback amounts. Regions that use the VisaNet Cashback Service can control member and country participation, and can set maximum cashback limits and different pricing options by country.

Acquirers and acquirer processors in the U.S. region, and those in the AP and LAC regions with merchants in U.S. territories, that process Visa and Interlink POS transactions with cashback must support partial authorizations.

V.I.P. 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 cashback transaction is domestic. The cashback amount field is Field 61.1—Other Amounts. If the transaction is non-domestic, V.I.P. converts cashback amount in field 61.1 to the issuer currency code and forwards the converted amount in field 61.2 to the issuer.

Table 1-4 lists the cashback services currently supported by VisaNet.

Table 1-4 Cashback Services Currently Supported by VisaNet

Cashback Service	Region	Cards	Maximum Amounts
VisaNet Cashback Service	Asia-Pacific, CEMEA, Visa Europe (in progress)	Visa, Visa Electron	Defined by regions, countries
U.K. Cashback Service	United Kingdom only	Visa, Visa Electron	Defined by merchant, cardholder, and issuer

V.I.P. System Services, Volume 2, contains a complete service description. Regions interested in the service can contact their Visa representatives for details about participation.

1.6.22 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 U.S. 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$499,999.99 for Visa Signature, Visa Signature Preferred, Visa Infinite, or 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.
- USD$499,999.99 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 Commercial card large-ticket POS transactions under USD$100,000.00 using issuer-specified processing rules. Refer to “Editing Transaction Amounts” in Chapter 3 for further information.

1.6.23 Visa Personal Payments

Visa Personal Payments is a product platform that delivers funds to Visa accounts using the original credit transaction (OCT). This platform supports multiple applications of the OCT, including money transfers, funds disbursements, credit card bill payments, and prepaid loads. All Visa Personal Payments services use the enhanced format for 0200 full financial OCTs. The Visa Personal Payments platform does not apply to the Visa U.S.A. region. For further details, contact your Visa representative.

V.I.P. declines cross-border-enhanced OCTs that have a business application identifier of **CP** (credit card bill payment) with response code **93** (transaction could not be completed—violation of law).

In cross-border money transfer-enhanced OCTs, the optional issuer fee (OIF) is not deducted from the amount that the recipient receives.

1.6.24 Visa POS Offers Redemption Platform (VPORP)

The Visa POS Offers Redemption Platform, or VPORP, is a VisaNet feature that provides offer redemption capabilities at the time of transaction authorization. This processing applies only to U.S. domestic transactions.

Visa assigns specific MVVs to participating merchants. These merchants submit offer details to Visa. Cardholders can enroll for POS offer redemption processing, and can register for specific offers. When a cardholder uses an enrolled card at a point-of-service and the transaction meets an offer’s requirements, Visa applies the applicable discount to the transaction amount in field 4, and sends the transaction to the issuer for authorization. VisaNet returns the issuer’s authorization response to the merchant with additional offer-specific details appended. Cardholders may subscribe to alerts to receive specific details of the offers that are applied to their transactions.

VPORP processing applies to 0100 authorization requests and their responses. VisaNet supports fully discounted transactions (transactions in which the field 4 value is reduced to zero). Fully discounted transactions are not sent to issuers.

1.6.25 Visa Product Eligibility Inquiries

Visa *product eligibility inquiries* provide consumer and commercial product information associated with the cardholder's account number. V.I.P. does not forward these requests to issuers. V.I.P. bases its responses on card-level information or on account range details that V.I.P. retrieves from the system files. These 0100 authorization requests and 0110 responses are non-financial, information-only transactions. Product eligibility inquiries are valid for BASE I and SMS POS.

The key product eligibility inquiry fields in 0100 authorization request are:

- Field 3—Processing Code: Positions 1–2, must contain **39** to indicate a product eligibility inquiry.
- Field 4—Amount, Transaction: The field must contain **zero**. If the acquirer sends a different amount, V.I.P. changes it to **zero**.
- Field 25—POS Condition Code: The code must be **51** for verification only.

0110 responses include the key field, Field 62.23—Product ID. V.I.P. populates this field with card product identification information from the Cardholder Database, the system files, or both.

Acquirers must test for the codes in field 3 and field 25, along with their ability to receive and process field 62.23. Participation is limited. Members can contact their Visa representatives for complete details.

1.6.26 Visa Smart Debit/Smart Credit (VSDC)

Visa Smart Debit/Smart 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 cardholder's chip card and the terminal and do not go through VisaNet. VisaNet 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 issuer's cryptogram in the 0110 authorization response to ensure that the issuer that created the card is the issuer that approved the transaction. If V.I.P. performs processing for the Card Authentication feature on behalf of the issuer, V.I.P. validates the Authorization Request Cryptogram (ARQC) and provides the Authorization Response Cryptogram (ARPC) in the response. If the issuer participates in the Issuer Authentication feature, either the issuer or V.I.P. generates a cryptogram (Authorization Response Cryptogram) 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.

NOTE

U.S. POS acquirers and acquirer processors must support contact and contactless chip cards and must be able to carry full chip data in field 55.

BASE I 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).

V.I.P. processes VSDC transactions according to card type. VisaNet supports the following card types:

Visa Integrated Circuit Card Specification (VIS)—This card type uses the initial Visa chip card type specifications for communicating between EMV (JCB, MasterCard, Visa) cards and their issuer processors.

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 VisaNet. V.I.P. 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 Positive Authorization Capacity Management (PACM) Service processing, Positive Cardholder Authorization Service (PCAS) processing, and STIP. The following are issuer-optional V.I.P. actions for a VSDC transaction when the issuer has specified “route to issuer” in the system tables:

- If PACM parameters indicate “perform STIP,” V.I.P. sends the transaction to STIP.
- If PCAS parameters indicate “perform STIP,” V.I.P. 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, V.I.P. sends the transaction to available issuers.
- If issuers are unavailable, V.I.P. reroutes the chip transactions to STIP, which applies issuer-specified processing parameters.

VisaNet always sends Generic EMV Transport transactions to available issuers or declines them in STIP if the issuer is unavailable.

V.I.P. supports chip cards having an alternative primary account number (PAN) stored on the chip. This PAN is different from the PAN embossed on the card, and serves as a security measure to prevent counterfeit chip cards from being used for non-chip transactions. Alternative PAN processing applies to VIS, CCD, and Generic EMV Transport cards, and to all cryptogram version numbers (CVNs) supported. V.I.P. account ranges can be set up to indicate alternative PAN support. V.I.P. declines a transaction with response code **59** (suspected fraud) if all of the following apply:

- The account range of the card indicates that it supports an alternative PAN.
- Field 22 does not contain **05**, **07**, **91**, or **95**.
- Chip data is not present in field 55 or the third bitmap fields.

For further information, refer to the VSDC Service description in *V.I.P. System Services, Volume 1*, and to the *Visa Smart Debit/Visa Smart Credit System Technical Manual*, doc ID 6001-04.

1.6.26.1 Visa iCVV Convert

The *Visa iCVV Convert Service* validates and converts a chip-based transaction to appear as a magnetic stripe-based transaction. VisaNet validates the cryptogram, removes unnecessary chip data, and submits the authorization request to participating issuers. Issuers can participate in this service optionally. Visa iCVV Convert is available both for BASE I and SMS users, and also supports contactless chip transactions.

- Field 55—Integrated Circuit Card (ICC)-Related Data is removed.
- Field 23—Card Sequence Number is removed.
- Field 44.8—Card Authentication Results Code is removed.
- Field 60.3 (Chip Condition Code), Field 60.6 (Chip Transaction Indicator), and Field 60.7 (Chip Card Authentication Reliability Indicator) are zero-filled, or dropped, if no subsequent field 60 subfields are present.
- Field 39—VisaNet does not send Online CAM authentication results (response code **82**), and offline approval (**Y1**, **Y3**) or decline (**Z1**, **Z3**) response codes to participating issuers—VisaNet converts **Y1** and **Y3** to **00** (Approved) and **Z1** and **Z3** to **05** (Do not honor) before sending them to participating issuers. However, the response codes **Y1**, **Y2**, **Z1** and **Z3** are sent in 0120/0220 advices to participating issuers. CVV results are sent in field 44.5.

If the issuer participates in Visa iCVV Convert and the transaction passes Online Card Authentication Method (Online CAM), VisaNet replaces the iCVV present in the track data (field 35 or field 45) with a VisaNet-generated CVV. In such instances, iCVV checking is not performed. However, If the issuer participates in Visa iCVV Convert, but the transaction fails Online CAM, VisaNet declines the transaction with a response code value of **05** (Do Not Honor) in field 39.

If chip data for Online CAM validation is not present in the request message, VisaNet performs iCVV validation. If the transaction passes iCVV validation, VisaNet replaces the iCVV present in the track data (field 35 or field 45) with a VisaNet-generated CVV. However, if the transaction fails iCVV validation, VisaNet declines the transaction with response code **05** (do not honor).

VisaNet declines the transaction with response code **05** (do not honor) if the issuer participates in Visa iCVV Convert, but the issuer's MDK (Online CAM) and CVK (CVV) are not present.

1.6.26.2 VSDC PIN Management Service

The Visa *VSDC PIN Management Service* allows Visa card cardholders to change or to unblock PINs in VSDC cards. Acquirers and issuers must successfully complete testing to participate in the service to provide the capability. Both must have successfully completed VSDC testing; 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 PACM processing or for STIP. If the issuer is unavailable or if the request times out, STIP responds with response code **91** in field 39.

V.I.P. does not include CVV or PVS PIN verification with PIN management processing, only PIN translation. However, VSDC PIN Management Service participants may also participate in the PIN Verification Service (PVS) and in the Card Verification Value (CVV) Service. Refer to *V.I.P. System Services, Volume 1*, for more information about the VSDC PIN Management Service.

The BASE I System and the VisaNet Network

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 2 BASE I Messages and Flows

This chapter describes the message format, structure, types, and sets that BASE I uses. It also explains how various types of BASE I messages flow among issuers, acquirers, and the V.I.P. System.

IMPORTANT

In the V.I.P. System 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 the V.I.P. System enforces edits and rejects transactions for some violations of mandatory requirements, V.I.P. does not enforce edits for* all *mandatory or conditional fields and values.*

*Visa strongly urges members and their processors to comply with mandatory field requirements. 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 also advises members not to rely on the V.I.P. System to reject **all** transactions that do not comply with mandatory or conditional requirements.*

2.1 MESSAGES

As mentioned in Chapter 1, two primary functions of the BASE I System are message *management* and message *routing*. To ensure that VisaNet processes and routes messages correctly, Visa has set standards for how members are to format messages. Issuers and acquirers format messages according to these Visa standards. BASE I edits messages for valid content and syntax before routing them to the issuer or to the stand-in processor (STIP) for authorization. BASE I also edits the response messages returned to the acquirer.

2.1.1 Message Format

Both BASE I and SMS support the V.I.P. message format. This format enables members to use both processing systems for their transactions as they prefer.

Each member designates which message format its processing centers use, and all of the member's messages must comply with that format. If message originators do not use the same format used by message recipients, BASE I automatically makes any necessary field adjustments before delivering messages to their destinations.

Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for details about the V.I.P. message format and field requirements.

2.1.2 Message Structure

Visa bases the V.I.P. message format 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 ensure that the messages conform to these standards, BASE I messages contain *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.

Table 2-1 illustrates the message elements that each bitmapped message contains.

Table 2-1 V.I.P. Message Structure

Message Header	Message Type Identifier	Bitmaps	Data Fields

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 data 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.
- Data Fields—A variable number of data 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 *tag-length-value (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, VisaNet users format almost every numeric field in packed format, which cuts the field length in half.

Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for detailed information about the message header, bitmaps, and data fields.

2.1.3 BASE I Message Types

BASE I 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 digitized voice prompts (for instance, through VoiceTec software). The terminal then generates the 0100 authorization request.

  NOTE

  The V.I.P. 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 International 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 the previous section, 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, cash disbursement, or Check Acceptance Service processing for several card products.

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

Table 2-2 BASE I Authorization-Related Message Types

Message Identifier	Message Type
	Cardholder Transactions
0100	ATM or U.S. POS Balance Inquiry Authorization Request Authorization Status Check Request Incremental Authorization Request Partial Approval Request Prepaid Activation Request Prepaid Activation and Load Request Prepaid Load Request Prepaid Partial Load Request Recurring Payment Request Recurring Payment Cancellation Request U.S. Bill Payment Request Verification Request (Account, Address, CVV2) **NOTE:** *When V.I.P. receives an AVS-only account verification request destined for a U.K. issuer that is directly connected to Visa Europe Authorisation Services, V.I.P. forwards the request to Visa Europe Authorisation Services, which determines whether the request is to be processed by its stand-in processing system or forwarded to the issuer.*

Table 2-2 BASE I Authorization-Related Message Types (continued)

Message Identifier	Message Type
0110	Authorization Response Authorization Status Check Response Balance Inquiry Response Incremental Authorization Response Partial Approval Response Prepaid Activation Response Prepaid Activation and Load Response Prepaid Activation and Partial Load Response Prepaid Load Response Prepaid Partial Load Response Recurring Payment Response Recurring Payment Cancellation Response U.S. Bill Payment Response Verification Response
0400	Partial Approval Reversal Reversal Request Reversal—Void of Activation Request Reversal—Void of Load Request
0410	Partial Approval Response Reversal Response Reversal—Void of Activation Response Reversal—Void of Load Response
System-Generated Transactions	
0120	Authorization Advice File Update Advice Discrepancy Advice
0420	Reversal Advice

Table 2-3 lists all BASE I non-authorization-related message identifiers and their associated message types.

Table 2-3 BASE I Non-Authorization-Related Message Types

Message Identifier	Message Type
	File Update Transactions
0300	File Update or Inquiry Request (Acquirer)
0302	File Update or Inquiry Request (Issuer)
0310	File Update or Inquiry Response (Acquirer)
0312	File Update or Inquiry Response (Issuer)
0322	File Update or Discrepancy Advice
	Administrative Transactions
0800	Network Management Request
0810	Network Management Response

Visa card transactions can consist of all of the BASE I message types shown in Table 2-2 and in Table 2-3. VisaNet limits other card transactions to the message types listed in Table 2-4.

Table 2-4 BASE I Card Types and Their Allowable Message Types

Card Type	Message Type	Comments
Plus	0100 Authorization Request 0110 Authorization Response 0100 ATM Balance Inquiry 0110 ATM Balance Inquiry Response 0120 Authorization Advice 0200 Alternative Media Request 0220 Misdispense 0400 Reversal Request 0410 Reversal Response 0420 Reversal Advice	n/a

Table 2-4 BASE I Card Types and Their Allowable Message Types (continued)

Card Type	Message Type	Comments
Visa Member Proprietary	0100 Authorization Request 0110 Authorization Response 0120 Authorization Advice 0400 Reversal Request 0410 Reversal Response 0420 Reversal Advice	For instance: Bank ATM card
Private Label	0100 Authorization Request 0110 Authorization Response 0120 Authorization Advice 0400 Reversal Request 0410 Reversal Response 0420 Reversal Advice	For instance: Discover card, JCB card, department store credit card
MasterCard	0100 Authorization Request 0110 Authorization Response 0100 Balance Inquiry Request 0110 Balance Inquiry Response 0400 Reversal Request 0410 Reversal Response	Includes Banknet
Travel & Entertainment (T&E)	0100 Authorization Request 0110 Authorization Response	U.S. region T&E cards include American Express, Carte Blanche, Diners Club
Check Acceptance	0100 Authorization Request 0110 Authorization Response	Vendors include Equifax Card Services (TeleCredit Los Angeles and TeleCredit Tampa), ETC/Scan (Deluxe Data Systems), JBS/NBC, State Street Bank, and TeleCheck **NOTE:** *Check Acceptance Service is a U.S. region-only service.*
SITA Airline Network	0100 Authorization Request 0110 Authorization Response	SITA transactions enable airline ticket agents to authorize Visa transactions without having to first call an acquirer.

2.1.4 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 V.I.P. 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 2-5 lists the BASE I cardholder transactions and their associated message sets.

Table 2-5 BASE I Cardholder Transactions and Their Message Sets

Cardholder Transactions	Message Set	Comments
Authorization or Confirmation for POS, ATM, Visa Smart Debit/Smart Credit (VSDC), Electronic Commerce, and Contactless	0100 Request 0110 Response 0120 Advice 0400 Reversal 0410 Response	Acquirers must NOT send confirmations to issuers for Visa card ATM or Plus international transactions for a misdispense.[1]
POS Account Number, Address, or Card Verification Value (CVV) Verification using a USD$0 Transaction Amount	0100 Request 0110 Response 0120 Advice	Acquirers cannot reverse verifications. **NOTE:** *When V.I.P. receives an AVS-only account verification request destined for a U.K. issuer that is directly connected to Visa Europe Authorisation Services, V.I.P. forwards the request to Visa Europe Authorisation Services, which determines whether the request is to be processed by its stand-in processing system or forwarded to the issuer.*
ATM or U.S. POS Balance Inquiry	0100 Request 0110 Response	Visa Smart Debit/Smart Credit (VSDC) inquiries include chip card authentication. Acquirers cannot reverse balance inquiries. POS balance inquiries can be stand-alone or can be part of an authorization request.
Check Acceptance	0100 Request 0110 Response	Acquirers cannot reverse check acceptance requests and STIP cannot process them.

[1] A *misdispense* occurs when the amount of the funds that a cardholder actually receives differs from the requested amount.

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

2.2 MESSAGE FLOWS

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

2.2.1 Authorization-Related Message Flows

Cardholders initiate authorization requests at a point of service or point of sale (POS) or at an ATM for a purchase or cash disbursement approval from the card issuer. Merchants and acquirers also use these requests for status checks; balance inquiries; account or address verifications; and check acceptance requests.

NOTE

When V.I.P. receives an AVS-only account verification request destined for a U.K. issuer that is directly connected to Visa Europe Authorisation Services, V.I.P. forwards the request to Visa Europe Authorisation Services, which determines whether the request is to be processed by its stand-in processing system or forwarded to the issuer.

NOTE

Visa Europe Authorisation Services can send 0100 account verification messages that contain Verified by Visa (VbV) authentication data. V.I.P. authenticates the CAVV and performs standard VbV processing on these messages before forwarding them to issuers.

2.2.1.1 Authorization Request (0100) and Response (0110) Message Flows

When BASE I receives an authorization request, it determines whether to forward it to the issuer or to STIP, based on routing parameters. See Chapter 4, BASE I Limits and Routing, for information about establishing these parameters.

Figure 2-1 shows the typical authorization request message flow for an authorization request for a Visa, proprietary, or private-label card transaction when VisaNet 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 VisaNet follow all of the transaction's processing rules.

NOTE

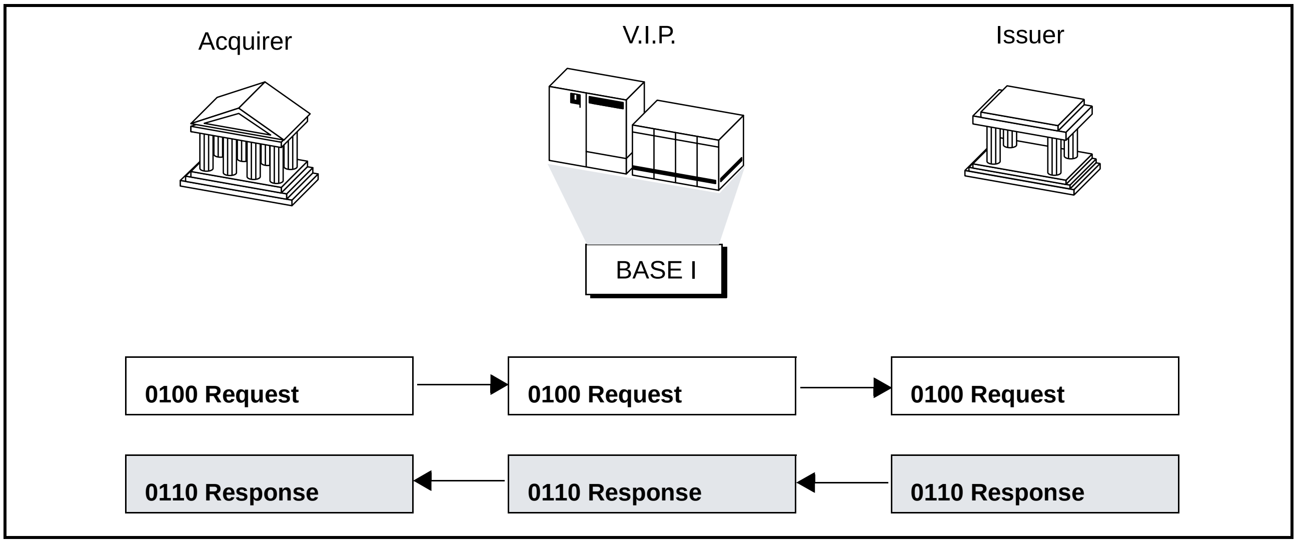
BASE I issuers can choose to receive authorization request messages with time limits in Field 63.2—Time (Preauth Time Limit). The time limit notifies the issuer the time by when the merchant or acquirer intends to complete the transaction. Issuers choosing to receive field 63.2 must send the field in response messages.

U.S. issuers who do not choose to receive field 63.2 receive 0100 authorization requests with the estimated amount, but without field 63.2. These preauthorization requests are for amounts exceeding USD$1.00.

IMPORTANT

Issuers connected to BASE I must be prepared to receive Field 63.2—Time (Preauth Time Limit) in 0100 preauthorization request messages. Although it is currently optional for issuers to receive this field, migration to SMS will require isssuers to support Field 63.2. Issuers will then be able to use Field 63.2 to identify that the 0100 message is a preauthorization request.

Figure 2-1 Authorization Request Message Flow—BASE I

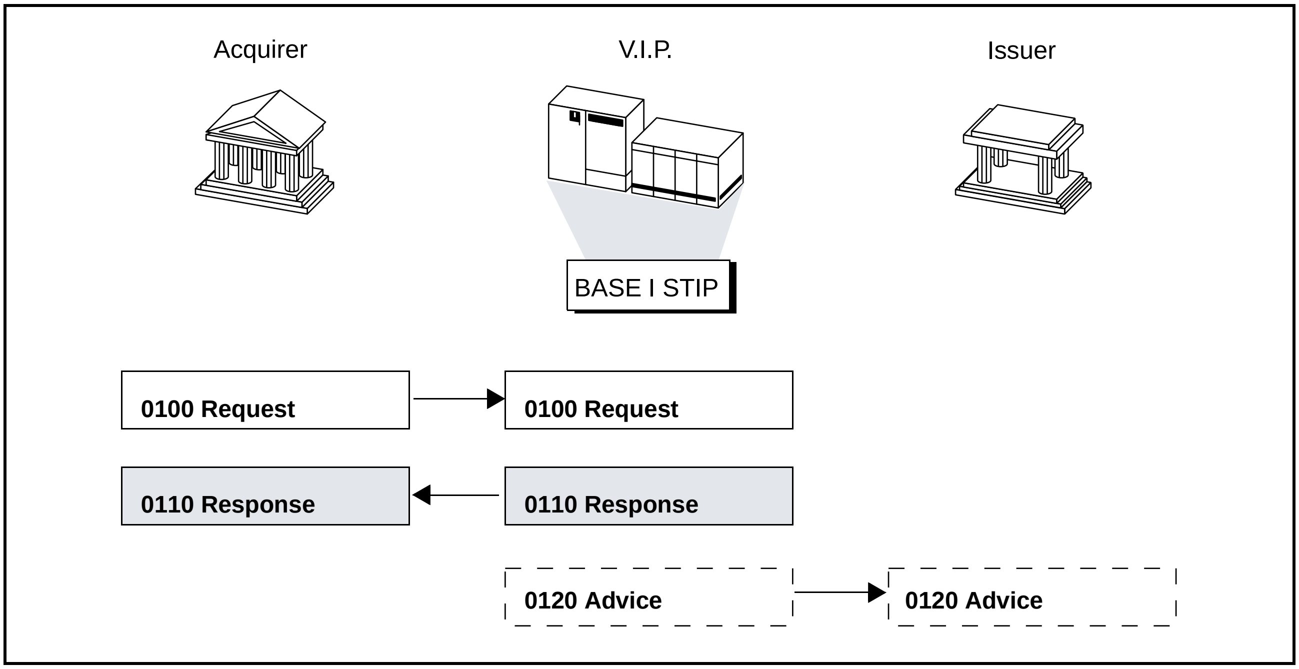


BASE I drops Field 20—PAN Extended, Country Code from 0100 POS and ATM authorization messages before sending them to the issuer. BASE I also drops this field from 0110 authorization responses before sending them to the acquirer.

BASE I rejects 0100 authorization request messages that contain an invalid value in Field 33—Forwarding Institution Identification Code with reject code **0057** (Invalid value).

Figure 2-2 illustrates the message flow when STIP processes the transaction. In this case, BASE I STIP responds on behalf of the issuer and creates an 0120 advice for the transaction. If the issuer is unavailable or V.I.P. 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, refer to Chapter 5, Stand-In Processing (STIP).

Figure 2-2 Authorization Request Message Flow—BASE I STIP



Acquirers and issuers must respond to STIP authorization advices with response code **00** in field 39. BASE I rejects 0130 STIP authorization advice responses that don't contain response code **00** with reject code **0590** (Invalid value (not **00** or **55** when it should be)).

BASE I forwards responses from issuers to acquirers. When BASE I is unable to return a response (for instance, if the acquirer processor is down), BASE I logs and discards the response. The acquirer then resends the authorization request.

NOTE

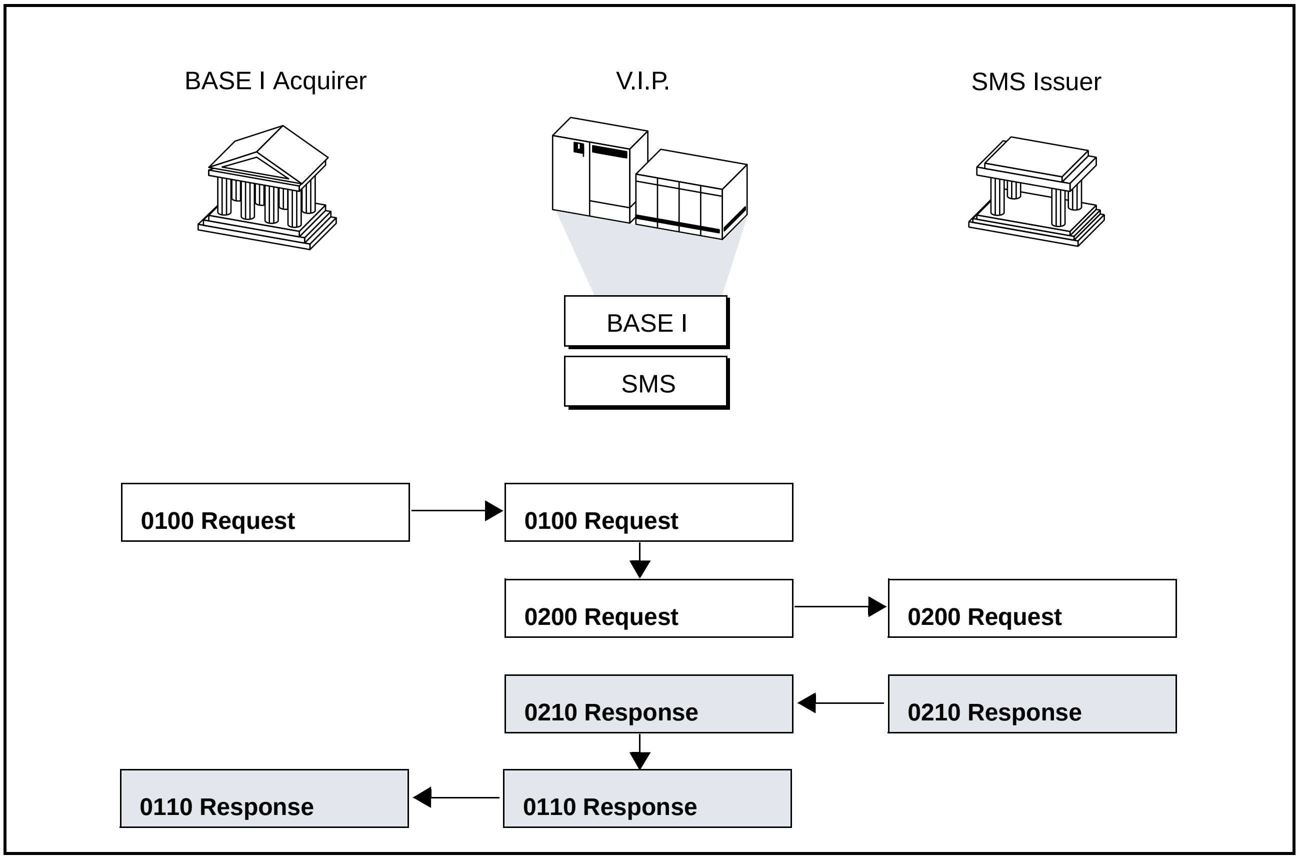
Visa U.S. BASE I issuers receive U.S. domestic Interlink-acquired original transactions as 0100 messages if they have account ranges set up to process PIN-authenticated POS transactions.

2.2.1.2 Transactions Between BASE I Acquirers and SMS Issuers

V.I.P. 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 V.I.P., which converts it to an 0110 message and forwards the response to the BASE I acquirer. V.I.P. 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 2-3 illustrates a typical authorization request message flow between a BASE I acquirer and an SMS issuer when the issuer participates in the ATM Format Conversion Service.

Figure 2-3 ATM Authorization Request Message Flow Between a BASE I Acquirer and an SMS Issuer That Participates in the ATM Format Conversion Service



2.2.1.3 Balance Inquiries

VisaNet supports both international ATM balance inquiries and international POS balance inquiries.

Support for ATM balance inquiries is mandatory for U.S.-region acquirers. Support for POS balance inquiries is mandatory for U.S.-region acquirers (except for Interlink acquirers). Support for both ATM and POS balance inquiries is optional for acquirers in all other regions.

2.2.1.4 ATM Balance Inquiries

Acquirers within the U.S. region 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.

In the U.S. region, SMS acquirers can submit cardholder account balance inquiries to BASE I issuers that want to receive them. Issuers establish settings at the BIN level to indicate whether a specific center can receive SMS balance inquiries.

Support for ATM balance inquiries is mandatory for acquirers in the U.S.-region. It is optional for acquirers in all other regions.

When submitting a balance inquiry, SMS acquirers use 0200 financial transactions containing Processing Code **30**—Available Funds Inquiry in positions 1–2. V.I.P. converts the 0200 message to an 0100 message and forwards it to the issuer-processing center.

NOTE

VisaNet does not allow Field 4—Amount, Transaction in balance inquiries. If the field is present, V.I.P. rejects the message.

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.

2.2.1.5 POS Balance Inquiries

POS balance inquiries are available only in the U.S. region. Acquirers can submit supporting POS balance inquiries as stand-alone 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, BASE I POS balance inquiries do not require a PIN.

Support for POS balance inquiries is mandatory for acquirers (except for Interlink acquirers) and for issuers for U.S.-domestic transactions; transactions acquired in U.S. territories are not eligible. Support for POS balance inquiries is optional for all other regions.

Participating issuers can optionally return positive or negative balance information in field 54 in responses to stand-alone or purchase requests. Participating merchants print balance data on the cardholder's receipt. V.I.P. 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) V.I.P. 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 stand-alone POS balance inquiries. V.I.P. declines transactions with response code **57** (transaction not permitted to cardholder) in Field 39—Response Code. If the issuer is unavailable for a stand-alone POS balance inquiry, V.I.P. declines the transaction with response code **91** (issuer unavailable) to the acquirer.

NOTE

VisaNet does not allow field 4 in balance inquiries. If the field is present, V.I.P. rejects the message. VisaNet does not allow 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 Chapter 1 in *V.I.P. System BASE I Technical Specifications, Volume 1*.

2.2.1.6 MasterCard Authorization Requests

VisaNet routes MasterCard authorization requests to Banknet. VisaNet sends non-PIN-based and PIN-based POS MasterCard requests to Banknet. BASE I declines attempts to submit PIN-based ATM requests to Banknet with response code **81** (cryptographic error found) in field 39.

BASE I automatically converts messages from V.I.P. format to the MasterCard format during message routing. VisaNet converts V.I.P.-format requests received from acquirers to the MasterCard format and routes them to the MasterCard Banknet network. Banknet returns the responses, and VisaNet automatically reconverts the messages to V.I.P. format and forwards the responses to the acquirers.

Acquirers processing MasterCard transactions through VisaNet 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, V.I.P. 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 include the transmission date and time in Field 7—Transmission Date and Time, and postal code in Field 59—National Point-of-Service Geographic Data.

Acquirers that process MasterCard transactions must use either field 62.17 or field 104, usage 2 to submit MasterCard Trace ID in incremental authorization, reversal, and reversal advice 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 and reversal advice messages must also contain this field.

The Credit Gateway to Banknet handles such MasterCard services as Card Verification Code 2 (CVC2), MasterCard's version of the Visa Card Verification Value 2 (CVV2) Service. Refer to the Card Verification Value 2 (CVV2) Service chapter in *V.I.P. System Services, Volume 2*, for more information.

NOTE

Acquirers that process MasterCard transactions through VisaNet in the U.S. region must support new financial network codes in field 62.17. Refer to V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1*, for network codes and requirements.*

For details about how the gateway function transfers data between network formats, refer to the *Credit Gateway Service Cross-Reference Guide*. This document includes field-by-field data transfer descriptions between VisaNet-format dual-message 0100 authorization requests and responses, and American Express- and MasterCard-format authorization requests and responses.

2.2.1.7 Discover Authorization Requests

VisaNet authorizes Discover transactions and routes them through the Discover Gateway for processing. The messages do not require formatting because Discover transactions use the VisaNet message format. VisaNet delivers the request to the issuer's authorization center for approval and returns a response to the member or to the merchant by the reverse path. If the Discover issuer is unavailable, BASE I STIP can check card pick-up lists and cardholder activity, and can generate responses and advices based on the results of the checks.

V.I.P. forwards Field 116—Card Issuer Reference Data in 0110 approval responses that are generated by Discover. However, V.I.P. does not add this field to STIP approvals or messages containing non-approval response codes.

V.I.P. 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, V.I.P. includes the ID in the 0110 response message it returns to acquirers.

V.I.P. 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, V.I.P. overlays any acquirer-provided value in positions 32–42 in Field 90—Original Data Elements with a default value assigned by Discover.

Discover issuers store terminal identifiers and other information in the Merchant Central File (MCF) and can use the Merchant Central File Service (MCFS) to add, delete, or change information in the database. Discover issuers and acquirers in the U.S. region and in the United Kingdom have the option to participate in the Address Verification Service (AVS).

VisaNet supports the processing of Discover's Cardholder Identification Data (CID) values, which is Discover's version of the Visa Card Verification Value 2 (CVV2) program. VisaNet 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. See Chapter 25, Card Verification Value 2 (CVV2) Service, in *V.I.P. System Services, Volume 2*, for information about the CVV2 Service.

If issuers populate Field 62.17—Gateway Transaction Identifier, and if the Discover acquirer can receive Bitmap 62 and chooses to receive field 62.17, VisaNet forwards the field and its contents to the acquirer in the response message.

VisaNet provides reversal processing for Discover transactions. V.I.P. does not add field 116 to reversals.

2.2.1.8 Plus Transactions

The *Plus Program* is an ATM card program available to Visa members worldwide. Plus System, Inc. provides ATM interchange for cards bearing the PLUS logo.

Plus transaction flows are the same as those for Visa transactions. Issuers can choose BASE I and BASE II 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 *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, and to *V.I.P. System SMS ATM Technical Specifications, Volume 1 and Volume 2*.

2.2.1.9 Check Acceptance Requests

BASE I sends check acceptance requests directly to check acceptance vendors, such as Equifax and TeleCheck. STIP does not process these requests. If the vendor is unavailable, BASE I returns a response message to the acquirer with response code **91** (issuer unavailable) in field 39. Check acceptance requests (except Visa and Visa Electron card transactions) that contain response code **10** in Field 25—Point-of-Service Condition Code indicate that the customer's identification has been verified for those transactions. Merchants clear and settle approved checks through their normal check-clearing systems.

The Check Acceptance Service is only available in the U.S. region. Refer to *V.I.P. System Services, Volume 1*, for more information about the Check Acceptance Service.

2.2.1.10 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 customer 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, an account number verification request, or a check acceptance transaction.

Refer to “How V.I.P. Processes Repeat, or Duplicate, Authorization Requests” in Chapter 3 for further information about timed-out messages.

Figure 2-4 shows the typical message flow for an authorization reversal request.

Figure 2-4 Authorization Reversal Request Message Flow—BASE I

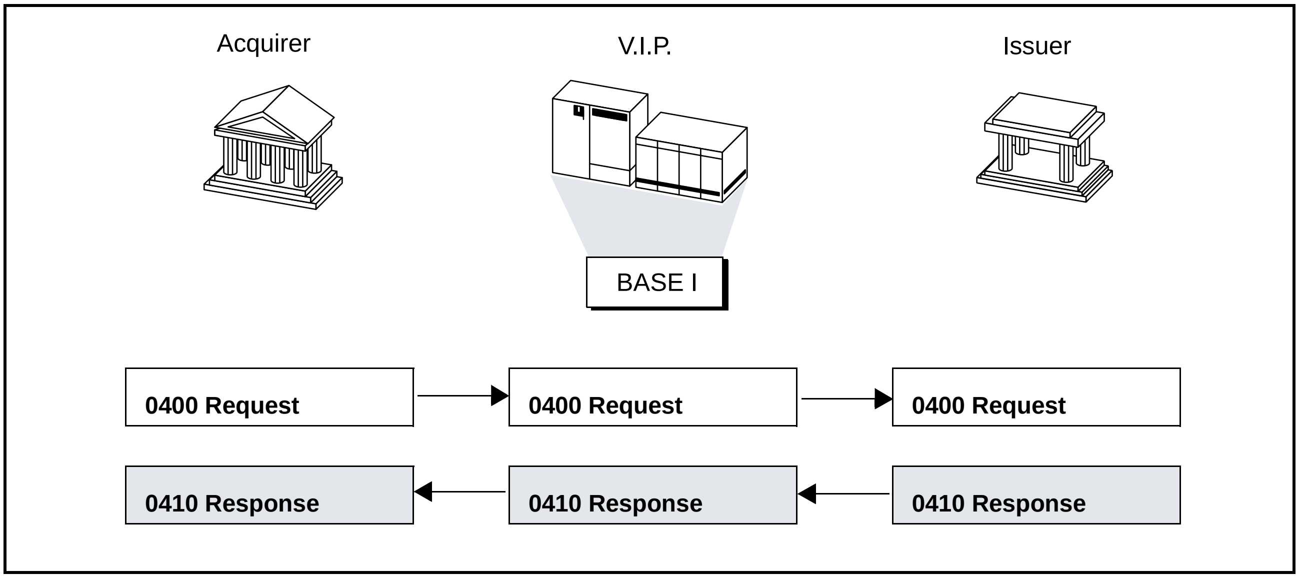


Figure 2-5 shows the message flow for an authorization reversal request processed by BASE I STIP.

BASE I drops Field 20—PAN Extended, Country Code from 0410 and 0430 responses before sending them to acquirers.

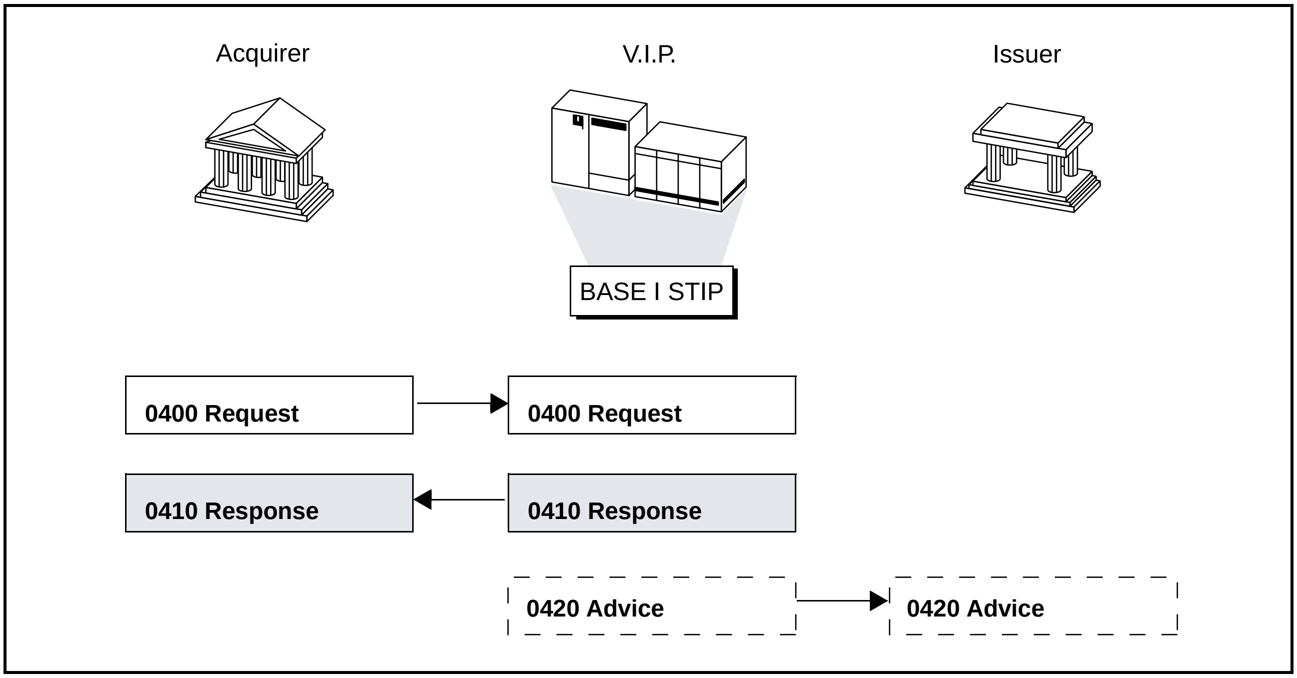
BASE I Messages and Flows

BASE I rejects 0400 reversals, 0400 partial reversals, and 0420 reversal advices that contain an invalid value in Field 33—Forwarding Institution Identification Code with reject code **0057** (Invalid value).

Field 38—Authorization Identification Response is conditionally present in 0400 reversals, 0400 partial reversals, and 0420 reversal advices. BASE I does not always send this field to issuers in these messages.

Acquirers and issuers must respond to reversals, partial reversals, and reversal advices with response code **00** in field 39. BASE I rejects 0410/0430 advice responses that don't contain response code **00** with reject code **0590** (Invalid value (not **00** or **55** when it should be)).

Figure 2-5 Authorization Reversal Request Message Flow—BASE I 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.

When 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; issuers must submit a file update message to adjust activity totals in the Cardholder Database at the VIC. See Chapter 5, Stand-In Processing (STIP), for more information about reversal processing and about activity checking.

When issuers process reversals, they should adjust available cardholder balances.

NOTE

*Visa U.S. BASE I issuers receive Interlink reversals for U.S. domestic transactions with a value of **01** in field 90.*

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, BASE I inserts the converted transaction amount in field 6 of the reversal. If the rates change, BASE I inserts the corrected, actual amount in billing currency into Field 61.2—Other Amount, Cardholder Billing of the reversal request.

NOTE

V.I.P. converts 0420 SMS full financial reversal messages to 0400 reversal requests for BASE I 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, BASE I 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, BASE I 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, BASE I inserts the converted original amount in field 6 and inserts the corrected replacement amount, if the currency rates have changed, in field 61.2.

2.2.1.11 ATM Confirmation (0102) Messages

Acquirers can no longer send ATM confirmations to fully or partially reverse ATM transactions. V.I.P. rejects them with Reject Code **0559**—Invalid Message Type. Acquirers must use 0400 reversal messages to fully or partially reverse ATM transactions.

2.2.2 Non-Authorization-Related Message Flows

BASE I, issuers, and acquirers use non-authorization messages for file maintenance, for administrative requests, and for network management.

2.2.2.1 Online File Maintenance Request (0120 and 0300/0302) and Response (0130 and 0310/0312) Message Flows

Acquirers and issuers can use online file maintenance messages to maintain their files stored in system files. There are two types of file maintenance messages:

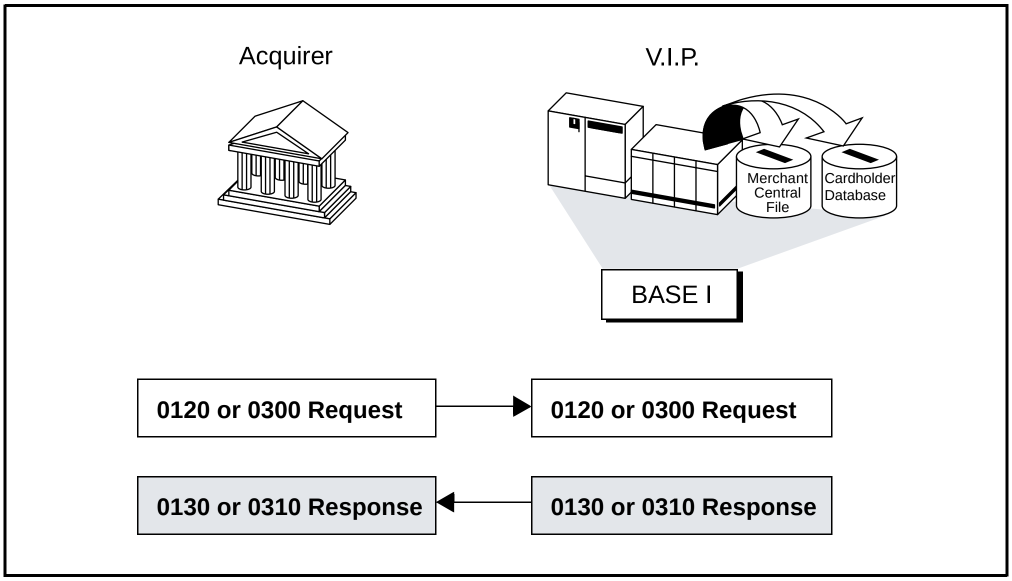
File Update—Members use file updates to add, to change, or to delete information in a file.

File Inquiry—Members use file inquiries to request data from a file.

BASE I 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. Acquirers use online file maintenance messages to update and to review records in the Cardholder Database and in the Merchant Central File. File maintenance messages can include information for MasterCard, Discover, American Express, and check acceptance accounts.

Figure 2-6 illustrates the file maintenance message flow for acquirers.

Figure 2-6 File Maintenance Message Flow for Acquirers



Issuers are responsible for creating and for maintaining the information in several of the files in the Cardholder Database (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.
- Portfolio File.
- Risk-Level File.

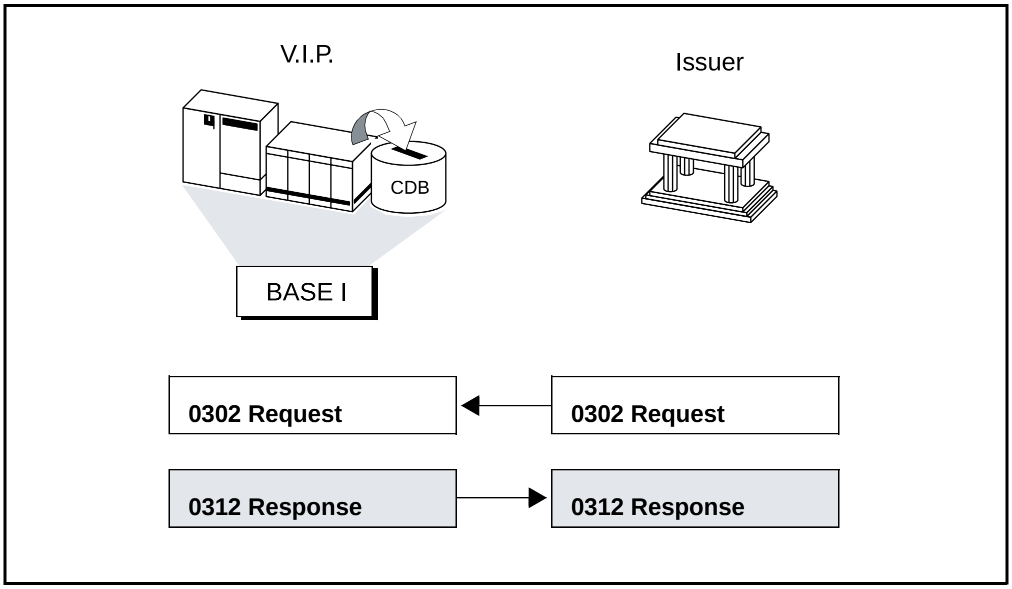
Depending on the region, issuers can update and request records contained in the Address Verification File.

V.I.P. can automatically update files in the Cardholder Database for participants in the Automatic Cardholder Database Update (Auto-CDB) Service, the Chargeback Reduction Service (CRS), or V-SAFE. Participants receive 0130 or 0322 file update advices when V.I.P. updates the Exception File on their behalf.

Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for more information.

Figure 2-7 illustrates the file maintenance message flow for issuers.

Figure 2-7 File Maintenance Message Flow for Issuers



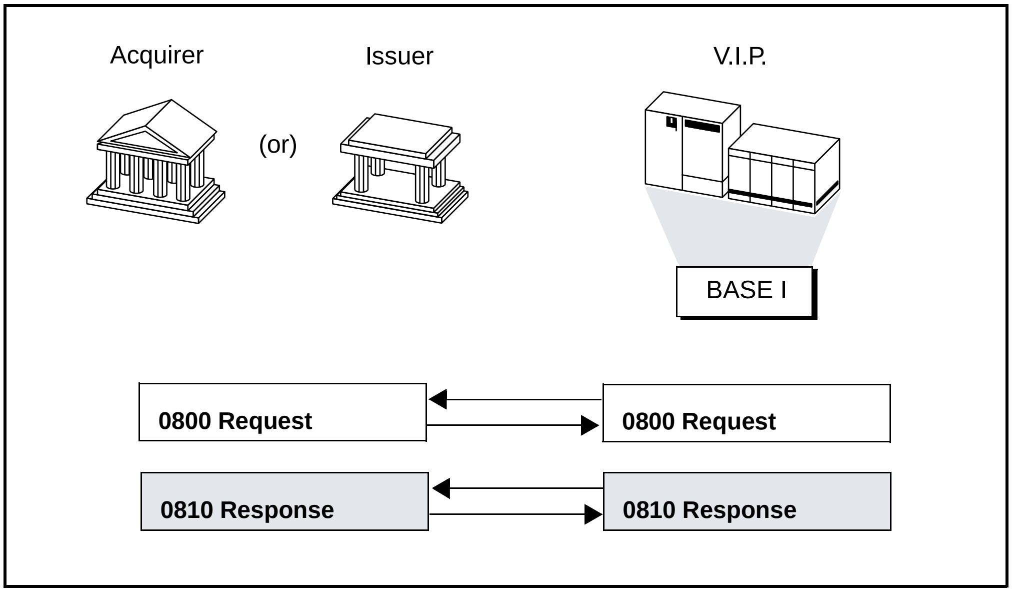
2.2.2.2 Network Management Request (0800) and Response (0810) Message Flows

BASE I uses network management messages for BASE I network management functions that control VisaNet access and message traffic. Network management functions include monitoring the operating status of members' processing centers. The member operating events or conditions that BASE I monitors include:

- Network sign-on.
- Test mode.
- Advice Recovery mode.

Figure 2-8 illustrates the network management message flow for network sign-on mode and for test mode.

Figure 2-8 Network Management Message Flow



Network Sign-On

BASE I uses 0800 and 0810 network management messages to communicate system status information between VisaNet and members and to initiate failure-recovery activities:

Sign-On—Issuers and acquirers use sign-on messages to notify BASE I 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 center has begun processing.

Sign-Off—Issuers and acquirers use sign-off messages to notify BASE I that they are unavailable to send and receive messages. Sign-off messages contain a value of **072** in field 70 that indicates that the center has stopped processing.

IMPORTANT

To recover from Sign-Off mode, Visa recommends that members sign their stations off from BASE I before they shut down their systems and sign on their stations to BASE I again to resume processing authorization requests.

Test Mode

Members that process BASE I and SMS messages using a common computer interface can also use 0800 network management request messages to test network communications. Processing centers insert a value of **301** in field 70 to test communications. V.I.P. uses the same messages to test network communications with processing centers as well.
If the V.I.P. request is a communications test, the recipient must acknowledge the request with an 0810 response message.

BASE I Messages and Flows

V.I.P. initiates test messages to members through their VisaNet connections during periods of inactivity to verify the members' connections. The frequency of the echo test messages are:

BASE I—Once per minute

SMS—Once every five minutes

SMS members can also choose to have V.I.P. send echo test messages at least once every five minutes regardless of traffic conditions whenever they are connected to VisaNet.

Advice Recovery Mode

By default, issuers remain in Advice Recovery mode indefinitely. Issuers that prefer to be in Advice Recovery mode only certain times of the day should use 0800 network management messages to sign onto or off Advice Recovery mode. Issuer stations can sign themselves on to BASE I Advice Recovery mode anytime by sending a network management message (0800) to BASE I. Once those issuers no longer want to receive advices, they should send an 0800 sign-off message to V.I.P.

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 BASE I an 0800 message with code **078**.
- The station can choose a more rapid advice-recovery process by prompting BASE I to send the next advice. To initiate rapid advice recovery, the station responds to each advice message, which causes BASE I to send the next advice immediately rather than waiting two seconds. If the response takes longer than two seconds to get to V.I.P., normal pacing of transmission resumes.

NOTE

Stations can also recover advices through the BASE II System rather than by using online messages. For information about BASE II advices, refer to BASE II documentation.

BASE I performs advice delivery once every second, and always starts at the top of its sorted station ID list. BASE I sends advices to the first station that is signed on in Advice Recovery mode. When the system delivers all stored advices to that station, BASE I begins sending advices to the next station in Advice Recovery mode.

BASE I stores advices in the advice file for a maximum of 15 days. If issuers do not recover their advices within 15 days, BASE I 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 BASE I creates them. Advice recovery does not interrupt authorization traffic.

NOTE

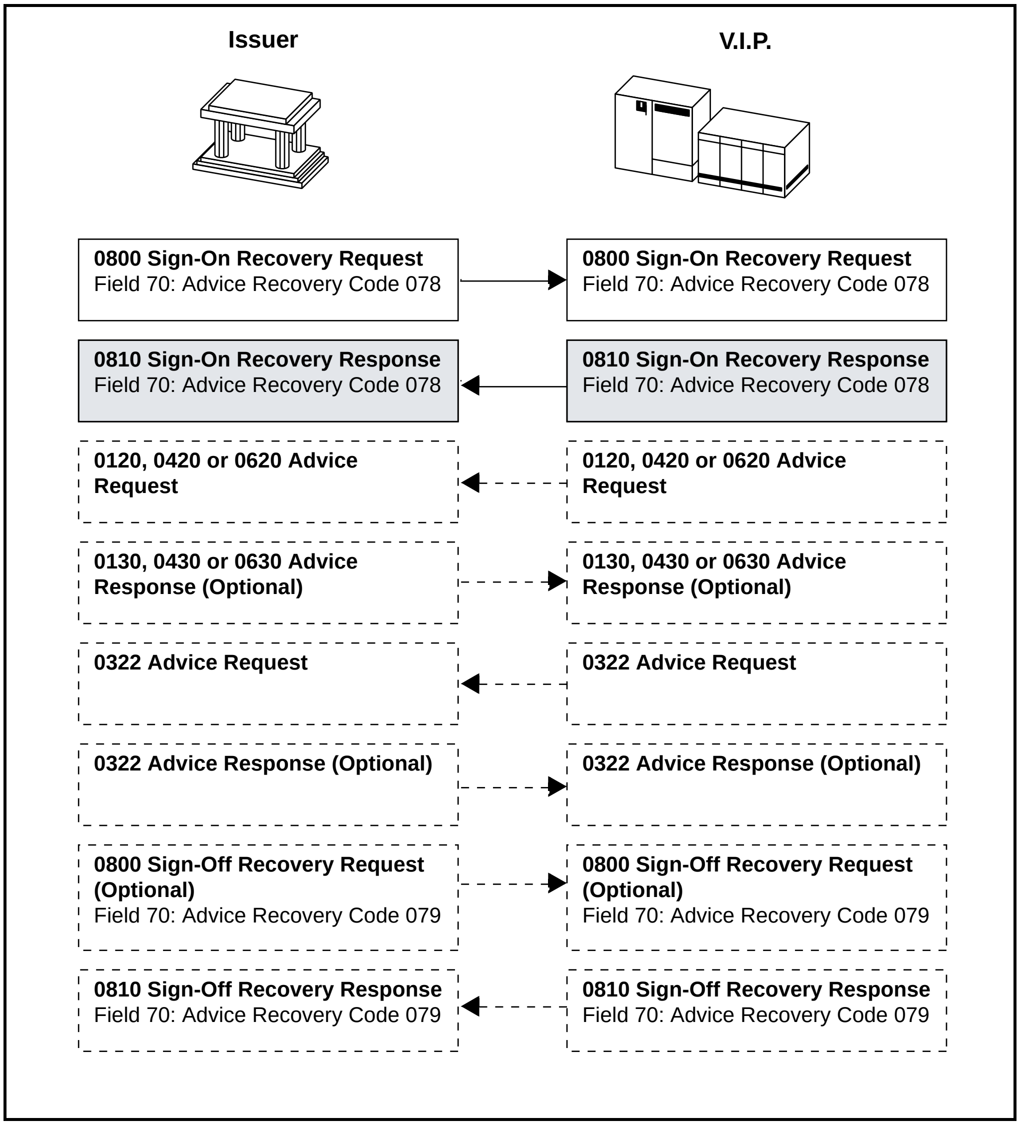
BASE I suspends advice recovery for issuers that participate in the Positive Authorization Capacity Management (PACM) Service when PACM is diverting transactions to STIP on their behalf.

Issuers and acquirers send advice recovery sign-off messages to indicate that they do not want to receive BASE I-generated advice messages. Centers 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 center uses the normal procedure to sign on again. Refer to the BASE I Advice Retrieval Service chapter in *V.I.P. System Services, Volume 2*, for a complete description of the service and its support for advice recovery.

Figure 2-9 illustrates the network management message flow for advice-recovery requests.

Figure 2-9 Advice Recovery Message Flow


Issuer
V.I.P.
0800 Sign-On Recovery Request
Field 70: Advice Recovery Code 078
0800 Sign-On Recovery Request
Field 70: Advice Recovery Code 078
0810 Sign-On Recovery Response
Field 70: Advice Recovery Code 078
0810 Sign-On Recovery Response
Field 70: Advice Recovery Code 078
0120, 0420 or 0620 Advice Request
0120, 0420 or 0620 Advice Request
0130, 0430 or 0630 Advice Response (Optional)
0130, 0430 or 0630 Advice Response (Optional)
0322 Advice Request
0322 Advice Request
0322 Advice Response (Optional)
0322 Advice Response (Optional)
0800 Sign-Off Recovery Request (Optional)
Field 70: Advice Recovery Code 079
0800 Sign-Off Recovery Request (Optional)
Field 70: Advice Recovery Code 079
0810 Sign-Off Recovery Response
Field 70: Advice Recovery Code 079
0810 Sign-Off Recovery Response
Field 70: Advice Recovery Code 079

2.3 HANDLING UNDELIVERABLE MESSAGES

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

2.3.1 Undeliverable Requests Ineligible for STIP Processing

When BASE I is unable to deliver an authorization request and cannot invoke STIP, it initiates a response containing response code **91** (issuer processor or switch inoperative). BASE I 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, or electronic commerce (MOTO/EC) transactions. When acquirers receive a response message containing response code **91**, they may retry the request or may use a downtime procedure (if the center has developed one). Centers 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 requires the following messages:

- 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, V.I.P. converts 0401 messages from BASE I acquirers to 0420 messages before forwarding them to SMS issuers.
- For ATM transactions, a reversal followed by a new request. (V.I.P. does not allow repeats for ATM transactions. V.I.P. 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, V.I.P. converts 0101 repeat messages from BASE I 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, V.I.P. converts 0101 repeat messages from BASE I 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. If BASE I acquirers send an 0101 POS request message 10 seconds after the original message has been processed, SMS issuers receive an 0101 request message.

NOTE

Acquirers should ensure that their merchants know to re-swipe the cardholder's 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.

2.3.2 Undeliverable Responses From Issuers

If BASE I cannot deliver an authorization or reversal response to an acquirer, it returns the response to the issuer. When BASE I 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.

Table 2-6 illustrates an example of a returned message.

Table 2-6 Returned Message Example

Header*	Type	Maps	Data Fields

* *BASE I 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 Assured Transaction Response (ATR), STIP then processes the transaction according to Assured Transaction Response (ATR) rules ATR settings.

If the issuer returns a response that does not contain matched Inter-Task Table (ITT) key fields from the original request, BASE I 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 ITT, V.I.P. rejects the response with Reject Code **0603**—Consistency Error Response and Request. STIP then processes the transaction according to Assured Transaction Response (ATR) settings.

NOTE

The Inter-Task Table (ITT) is an internal table within V.I.P. that V.I.P. uses to temporarily store messages so it can match requests to responses and monitor response times.

For further key field information, refer to “Adding the Message to the Inter-Task Table (ITT)” in Chapter 3, Message Validation and Routing Preparation, and to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*. Also refer to “How V.I.P. Processes Repeat, or Duplicate, Authorization Requests” in Chapter 3, Message Validation and Routing Preparation, for repeat or duplicate message processing information. Further ATR information is also located in Chapter 3, Message Validation and Routing Preparation.

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 3

Message Validation and Routing Preparation

The BASE I System 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 *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*. BASE I also performs any issuer-specified services such as adding Merchant Central File information or validating personal identification numbers (PINs).

The first functions that BASE I performs on requests from acquirers are listed below and are described in subsequent sections of this chapter. They apply to all authorization-related cardholder transactions processed by BASE I, including electronic commerce (e-commerce) transactions.

- Message source validation and message logging.
  - Verifying message source.
  - 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 the Merchant Central File Service (MCFS) or for the Custom Payment Service (CPS).
- Currency conversion.
- Adding messages to the Inter-Task Table (ITT) for tracking and response time purposes.
- Starting Positive Authorization Capacity Management (PACM) Service data accumulation, if the issuer is a participant. Otherwise, starting Positive Cardholder Authorization Service (PCAS) processing.
- Determining message destination.
- Determining message routing.
- Performing any magnetic stripe-based Card Verification Value (CVV), integrated chip card CVV (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 or PACM control, BASE I then routes the message to stand-in processing (STIP) or to the issuer. If the message is going to the issuer, BASE I starts the Assured Transaction Response (ATR) timer.

NOTE

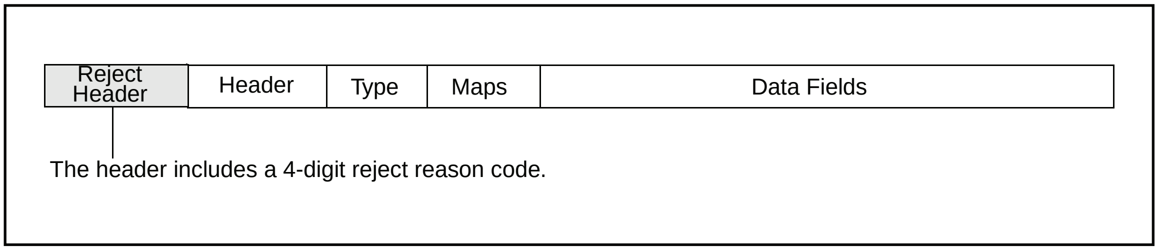
The ATR Service provides for additional response time for chip-based transactions.

If BASE I encounters a condition at any point in the process that precludes further processing, BASE I rejects or declines the message back to the acquirer or forward-refers the message to the issuer for disposition.

BASE I 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 BASE I 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 3-1.

Figure 3-1 Rejected Message Example



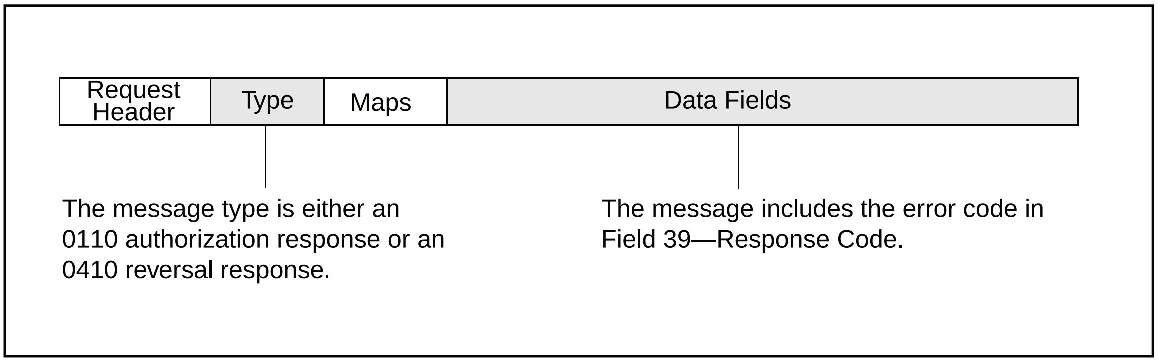
The reject header contains the standard header data plus two extra fields: a bitmap (in header field 13) and a 4-digit code (in header field 14) that identifies the reject reason. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for valid reject codes.

BASE I can reject a message from a processing center, but a processing center cannot reject a message originating from BASE I.

BASE I 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 card account number does not belong to any known issuer.

BASE I generates a decline response message, as indicated in Figure 3-2.

Figure 3-2 Decline Response Example


Request Header
Type
Maps
Data Fields
The message type is either an 0110 authorization response or an 0410 reversal response.
The message includes the error code in Field 39—Response Code.

V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2, identifies valid error decline response codes.

3.1 MESSAGE SOURCE VALIDATION AND MESSAGE LOGGING

When BASE I receives an authorization request, it uses information in the request along with information in the system tables to determine the originator of the request. The information includes:

Request Information	System Table Information
• Source Station ID (header field 6) • Acquirer's BIN (field 32) • Acquirer's country code (field 19)	• Acquirer VAP station address • Acquirer BIN Control Record (BCR) and Processing Center Record (PCR)

Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for detailed field descriptions.

3.1.1 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 BASE I uses in this process are:

- Field 19—Acquiring Institution Country Code
- Field 32—Acquiring Institution Identification Code (acquirer BIN)
- Field 33—Forwarding Institution Identification Code
- Field 43—Card Acceptor Name/Location

To determine the acquirer's country code, V.I.P. 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 V.I.P. compares it to the system's list of valid country codes, V.I.P. then uses the field 19 country code.

To determine the acquirer's region code, V.I.P. uses the field 19 country code. If field 19 is not present in the message, V.I.P. uses field 32 to locate the acquirer's BIN Control Record (BCR), and uses the default value in that BCR. If field 19 is not present, and the acquirer's BCR is not available, V.I.P. uses the acquirer's Processing Control 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, V.I.P. uses the country code in field 43. If field 43 is missing, the system uses the acquirer's region code.

NOTE

ATM cash disbursement authorization requests require fields 41, 42, and 43. For POS authorization requests, refer to the field 41, 42, and 43 field descriptions in V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for field presence requirements.*

For authorization requests that contain PIN data (in Field 52—Personal Identification Number [PIN] Data and in Field 53—Security-Related Control Information), V.I.P. 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.

Message Validation and Routing Preparation

V.I.P. routes transactions to issuers based on the account number range unless Field 100—Receiving Institution Identification Code (for check acceptance requests or for certain non-Visa card transactions such as MasterCard transactions processed in Malaysia), or Field 121—Issuing Institution Identification Code (for non-ISO-standard account numbers) is present. If present, V.I.P. uses the values in those fields for routing. Acquirers must first clear the use of those fields with Visa. See "Determining Message Destination" in this chapter.

So that billing processing can distinguish cross-border-issued transactions for Visa commercial card programs, BASE I always logs the BIN country as a point of comparison. For instance, a U.S. issuer that issued a card in France would have a BIN country code of **840** but an account range definition (ARDEF) country code of **250**; a card issued in the U.S. by that same U.S. issuer would have a BIN country code of **840** and no ARDEF country code.

3.1.2 Logging Messages and Performing Administrative Tasks

After BASE I validates the message's source, the system logs the request. BASE I logs each request and each response message to compile data for billing, preparing reports, recovering files, and researching problems. Generally, BASE I does not capture entire messages or maintain transaction histories; for instance, BASE I does not match entire reversals to entire original authorization messages.

There are three possible message-logging segments:

IR—Input Request from the member to the VisaNet Interchange Center (VIC)

IO—Input/Output with respect to the BASE I internal processing of a message

OS—Output Segment from the VIC to the member

BASE I logs only the IO segment unless full logging is active at the system or at the station level. *Full logging* means that BASE I logs all three segments. This functionality is only used to help members resolve a message transmission or a processing problem and to monitor messages between a member and the VIC.

Each VIC maintains its own log. System transaction logs are available for online viewing for six months by, for instance, the Visa Transaction Research Service (VTRS). After three years, VisaNet archives the logs.

3.2 MESSAGE PARSING AND PRE-ROUTING MESSAGE EDITING

The tasks involved with this phase of BASE I 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.
- Editing message fields.
- Performing Merchant Central File Service (MCFS), Visa Smart Debit/Smart Credit (VSDC) Service, or Custom Payment Service (CPS) functions, or validating a Cardholder Authorization Verification Value (CAVV) in an electronic commerce (e-commerce) request.

IMPORTANT

Field 55 may contain tags that the receiving issuer or acquirer does not recognize, or does not expect. The receiver must ignore such tags, and continue parsing the next tag in field 55.

(Refer to *V.I.P. System Services, Volume 2*, for information about PIN processing and about MCFS. For international CPS information, refer to the CPS ATM and CPS POS chapters in *V.I.P. System Services, Volume 2*. For U.S. CPS programs, refer to the latest edition of the *U.S. Interchange Reimbursement Fee Rate Qualification Guide*.)

3.2.1 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.

NOTE

V.I.P. 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 V.I.P. and its own processor perform verification, and when the issuer is available to verify PINS, V.I.P. performs PIN translation and forwards field 52 and field 53 to the issuer for PIN verification. When the issuer is unavailable, VisaNet forwards the two PIN fields to STIP for translation and verification.

If the issuer chooses to have V.I.P. perform PIN verification and if PIN verification is successful, V.I.P. drops field 52 and field 53 from the request message to the issuer.

3.2.2 Message Classification

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

BASE I 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.

BASE I rejects any message that is out of context (or out of sequence) to prevent it from being sent to issuers.

3.2.3 Obtaining Acquirer and Issuer Profiles

BASE I checks its system tables for member-defined processing parameters, such as the BIN Control Record (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 the Merchant Central File Service. BASE I uses this information to perform subsequent tasks. Chapter 4, BASE I Limits and Routing describes the Risky Countries feature. Refer to “Issuer Available and Unavailable Default Response Codes” in Chapter 5, Stand-In Processing (STIP), for a list of allowable default response codes that the issuer can specify.

3.2.4 Editing Message Fields

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

- Formatting, for instance, that the card expiration date is in *YYMM* format.
- Syntax, for instance, if a field requires a leading asterisk.
- Content, for instance, the value in Field 4—Amount, Transaction is zeros when it should contain an amount.
- Interfield relationships. BASE I compares different fields within a message to make sure that there is not any conflicting information.
- Service-specific field information. If, for instance, the acquirer subscribes to Custom Payment Service (CPS), BASE I validates the contents of Field 62—Custom Payment Service Fields.

When BASE I 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 BASE I 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 BASE I finds an error in one of the key CPS fields in a message being submitted for CPS qualification but the message is otherwise valid, BASE I 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, BASE I downgrades the request and processes it as a non-CPS-qualified transaction.

NOTE

V.I.P. assigns a transaction identifier (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 Custom Payment Service (CPS) consideration, including preauthorization messages and V.I.P.-format Plus transactions.*

Basic processing rules that govern authorization requests dictate BASE I 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
- Expiration dates

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

3.2.4.1 Editing Account Numbers

All POS and ATM card authorization messages require an account number. BASE I 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 the Track 2 data (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 and ATM transactions (network 0002). It does not apply to Plus ATM transactions (network 0004).

Typically, cardholder account numbers are unique ISO-standard account numbers that include the issuer ID in the first six positions. BASE I supports the following types of cardholder account numbers:

- 13- or 16-digit numeric bank card numbers. BASE I currently uses only the Luhn modulus-10 check digit algorithm to verify the check digit. Only STIP performs this verification.
- 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 cardholder account number. 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 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. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for details about using field 121. Members must prearrange the use of fields 102 and 103 with Visa, 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.

3.2.4.2 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.
- Check acceptance.
- Quasi-cash (for instance, a money order or a wire transfer).
- Available funds inquiry for the cardholder's account or credit balance.
- 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. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for detailed information about valid processing codes and about coding requirements.

NOTE

VisaNet does not support American Express Quasi-cash transactions.

3.2.4.3 Editing Magnetic Stripe and Service Restriction Code Data

BASE I checks to make sure that the card's magnetic stripe data appears in the Track 1 and Track 2 data fields of the authorization request. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, and to the *Payment Technology Standards Manual* for requirements for the contents of the track data in fields 35 and 45 in authorization request messages.

Service Restriction Code Check

BASE I also 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, BASE I 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, see the service code definitions in the *Payment Technology Standards Manual*.

3.2.4.4 Editing Transaction Amounts

Consumer Cards—For maximum amount limits on consumer POS transactions (that is, non-government, non-corporate, non-large-ticket), see the field 4 description in the *BASE I Technical Specifications, Volume 1*. The maximum amount includes charges and fees, such as optional issuer fees. Acquirers must contact issuers to obtain authorizations for larger transaction amounts. Issuers can establish higher limits for accounts listed the in Cardholder Database as having Very Important Person (**VIP**) status.

NOTE

All amounts are expressed in U.S. dollars.

Consumer Cards: Visa Infinite, Visa Signature, Visa Signature Preferred—For *consumer* (non-commercial large-ticket) Visa card transactions, the maximum amount is USD$499,999.99 including any fees and charges.

Commercial Large-Ticket: POS—USD$10,000,000.00 is the maximum amount, including any charges and fees, for U.S. government or non-government POS commercial large-ticket transactions. Transactions must be *U.S. domestic* (the transaction and issuer currency codes must be **840**). Acquirers must not specify a receiving institution ID.

- The card type for U.S. government General Services Administration (GSA) or Intra-Government Transfer System (IGOTS) transactions must be Visa Purchasing. Allowable merchant category codes for GSA large-ticket transactions are **3000–3999**, **4112**, **4411**, **4511**, **4722**, **5812**, **5814**, **7011**, and **7512**. The MCC for IGOTS transactions is **9045**.
- The card type for non-government commercial large-ticket transactions must be Visa Business, Visa Corporate (including Corporate Travel and Entertainment [T&E]), or Visa Purchasing (including Fleet). Commercial large-ticket transactions can also be initiated using Visa Infinite, Visa Signature, and Visa Signature Preferred cards if the issuing BIN is a commercial large-ticket participant and if amounts do not exceed the Visa Infinite, Visa Signature, and Visa Signature Preferred limitations.

Commercial Large-Ticket: Cash Disbursement—The maximum amount for U.S.-domestic commercial large-ticket cash disbursement transactions is USD$499,999.99. (The maximum amount for an individual clearing and settlement transaction is USD$500,000.00.)

T&E Transactions—The maximum amount for T&E transactions is USD$9,999,999.99, including any charges and fees. T&E transactions can be submitted as commercial large-ticket transactions if the issuing BIN is participating in the program.

- For the maximum amounts for Visa Signature, Visa Signature Preferred, Visa Infinite, and Visa Signature Business, see the field 4 description in the *BASE I Technical Specifications, Volume 1*.
- The maximum amount is US$9,999,999.99 for Visa Business, Visa Corporate, Visa Business Check Card, Prepaid Commercial, Visa Purchasing, Visa Purchasing with Fleet, Visa GSA Purchasing, and Visa GSA Purchasing with Fleet, when the ARDEF participation flag (large ticket) is **ON** for the card number.
- For the maximum amounts for 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, when the ARDEF participation flag (large ticket) is **OFF** for the card number, see the field 4 description in the *BASE I Technical Specifications, Volume 1*.

U.S. Tax Payments—For the maximum amounts for U.S. tax payments, refer to the field 4 description in the *BASE I Technical Specifications, Volume 1*. These transactions must be made with a Visa card, the MCC must be **9311**, field 63.1 must contain **0002**, and the Country Code subfield in field 43 must contain **US**. A valid merchant verification value (MVV) code must be present.

STIP does not process commercial large-ticket POS transactions between USD$99,999.99 and USD$10,000,000.00. VisaNet 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, (which allow additional response time for chip-based transactions). 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.

3.2.4.5 Editing Free-Text Data

Visa 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. BASE I 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.

3.2.4.6 Editing Expiration Dates

Except for check acceptance requests, all card-present authorization requests must contain a month and year card expiration date. For card-not-present transactions such as mail order, telephone order, or e-commerce (MOTO/EC), acquirers must enter the date in Field 14—Date, Expiration of the request message if:

- The expiration date is known.
- The issuer has set its BIN-level option to prevent requests from being processed without expiration dates.

V.I.P. considers a field 14 expiration date to be expired if it is 50 years greater than the current date.

Visa card issuers must use valid expiration dates. BASE I does not allow special substitute dates such as **1111** or **2222**. BASE I interprets the value **1111** as November 2011.

BASE I 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 expiration 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 BASE I issuers that lack an expiration date in field 14 but contain a magnetic stripe in Field 35—Track 2 Data, V.I.P. inserts the date from the magnetic stripe in field 14 in the message. Conversely, V.I.P. does not remove field 14 from requests from BASE I acquirers to SMS issuers that include track data.

Refer to Chapter 5, Stand-In Processing (STIP), for the procedures that STIP uses to determine the expiration date.

3.2.4.7 Performing Service- or Technology-Specific Processing

Depending on the member profile, BASE I executes the tasks for the Merchant Central File Service (MCFS), Visa Smart Debit/Smart Credit (VSDC) Service chip processing, Custom Payment Service (CPS), or the Visa Secure Electronic Commerce (VSEC) Service.

3.3 CURRENCY CONVERSION

BASE I can perform currency conversion when the transaction currency is different from the cardholder billing currency.

For Multicurrency Service participants, BASE I 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

BASE I adds the conversion rate it uses to the request. BASE I supports an XML-only message to convert the amount and return results to the Mobile gateway. The XML currency conversion request message contains a “source” Primary Account Number (PAN), a “destination” PAN, an amount, and a processing code. V.I.P. looks up the currencies associated with source PAN and destination PAN. It uses the source currency as the transaction currency and associates it with the amount submitted. V.I.P. then performs a conversion of the amount and source currency to the destination cardholder billing currency using the conversion rates associated with the transaction type as specified by the processing code.

For members that do not participate in the Multicurrency Service, BASE I converts amounts to U.S. dollars and omits the multicurrency fields.

NOTE

Some registered merchants can perform currency conversion locally, and they submit transactions in a cardholder's billing currency. 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. V.I.P. logs this field but does not send it to issuers.

Refer to the Multicurrency Service chapter in *V.I.P. System Services, Volume 2*, for a description of the service.

3.4 ADDING THE MESSAGE TO THE INTER-TASK TABLE (ITT)

The BASE I Inter-Task Table (ITT) 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 62.2—Transaction Identifier (TID)
- Field 63.1—Network Identification Code

BASE I 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 ITT. The ITT retains a transaction's key field information until the issuer or STIP sends a response to that transaction. Field 90—Original Data Elements is also one of the key message matching elements.

Acquirers must exercise caution if reusing field 37 values when submitting authorization requests. Refer to "Assured Transaction Response (ATR) Tracking" in this chapter for information.

Certain card type transactions require that the ITT 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.

NOTE

*For BASE I-acquired SMS transactions, SMS assigns reject code **0514** if it cannot match the response message in the ITT.*

3.4.1 Transaction Identifier (TID)

Field 62.2—Transaction Identifier is a key field used in message identification and matching. BASE I assigns a TID to all transactions.

BASE I assigns a TID to all 0100 authorizations and returns the TID to acquirers in all 0110 responses even if the issuer does not include it in the response.

Field 62.2 is mandatory in 0400 reversals (including partial reversals) and 0420 reversal advices. BASE I returns this field in 0410 and 0430 responses even if the issuer does not include this field in the response.

VisaNet does not send field 62.2 to gateway issuers. VisaNet returns field 62.2 to acquirers in gateway response messages.

3.5 STARTING PACM DATA ACCUMULATION

If the issuer participates in the Positive Authorization Capacity Management (PACM) Service, BASE I begins monitoring the issuer processor and accumulating traffic information.

3.6 DETERMINING MESSAGE DESTINATION

Visa 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. V.I.P. contains current records in what are called *account range routing tables*. BASE I acquirers must use Visa-supplied account range routing tables for ATM transactions. BASE I acquirers can at their discretion use Visa-supplied account range routing tables for POS transactions.

BASE I 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

BASE I also uses the issuer's profile from the system tables. The issuer's profile includes the BIN Control Record (BCR) and the Processing Center Record (PCR), the issuer's applicable account number ranges, and the issuer's country code.

BASE I uses field 2 or field 34 and field 100 to determine the destinations of check acceptance requests. Field 100 contains the check acceptance vendor routing code, for instance, **861400** (TeleCheck). Also, issuers can use field 33 or field 121 to route transactions to a designated BIN.

Issuers designate which of their processing centers 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 issuer. Optionally, issuers can control which processing center receives requests for their cardholders by designating multiple processing centers and specifying the types of transactions that should be routed to each processing center.

Visa 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 BASE II 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, refer to the Introduction to Routing Services chapter of *V.I.P. System Services, Volume 1*.

If the destination is a system or a network outside of VisaNet, BASE I has connections, or *gateways*, to outside systems and networks. V.I.P. 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 VisaNet connection point. Refer to the Gateway Services chapter of *V.I.P. System Services, Volume 1*, for detailed information about available gateways and Credit Gateway Services.

3.7 DETERMINING 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 PACM or PCAS processing rules. It also depends on the issuer's operating status, that is, whether the issuer is available or unavailable. Chapter 4, BASE I Limits and Routing, of this manual describes these subjects in detail.

3.7.1 Issuer Available and Issuer Unavailable Modes

An issuer processor is considered available if it has at least one station signed on to VisaNet. 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.

An issuer processor is considered unavailable if:

- The processor is not linked to VisaNet (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.

Refer to Chapter 4, BASE I Limits and Routing, for more information about issuer limits and about issuer-available and issuer-unavailable conditions.

3.7.2 Performing CVV or iCVV Verification

V.I.P. performs Card Verification Value (CVV) verification processing on the CVV 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. Depending on issuer specifications, V.I.P.:

- Validates the CVV or the integrated chip card CVV (iCVV) on all requests and forwards the results to the issuer in the request.
- Validates the CVV or the iCVV on all requests and if the validation fails, responds to the acquirer using the issuer's specified response code.
- Validates the CVV or the iCVV in a request only when the issuer is unavailable and it sends the request to STIP.

3.7.3 Performing Card Verification Value 2 (CVV2) Verification

If V.I.P. 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 V.I.P. 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 V.I.P. processing when both elements are present in a request, refer to the Card Verification Value 2 (CVV2) Service chapter in V.I.P. System Services, Volume 2*.*

3.7.4 Performing Cardholder Authentication Verification Value (CAVV) Verification

If issuers participating in the CAVV Verification Service have V.I.P. perform CAVV validation, V.I.P. 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, V.I.P.:

- 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, V.I.P.:

- 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, V.I.P. checks the value in Field 44.13—CAVV Results Code. If the value is **0**, which indicates that the CAVV authentication results are invalid, V.I.P. performs one of the following checks:

- If V.I.P. has the CAVV keys, and the CAVV results code validated by V.I.P. is not **0** (indicating that the first three positions of field 126.9 are valid), V.I.P. replaces the **0** value in field 44.13 with a valid CAVV results code and forwards the response message to the acquirer.
- If V.I.P. does not have the CAVV keys and V.I.P. determines that the first three positions of field 126.9 do contain valid values, V.I.P. 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 V.I.P. has the CAVV keys, and the CAVV results code validated by V.I.P. is **0** (indicating that the first three positions of field 126.9 are not valid), V.I.P. 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 honor).

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

3.7.5 Performing Dynamic Card Verification Value (dCVV) Verification

If V.I.P. performs dCVV validation for issuers that support contactless transactions, V.I.P. 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 V.I.P. validate the dCVV in all dCVV-eligible authorization requests.

3.7.6 PIN Translation and Verification

When V.I.P. receives a PIN-based authorization request for an issuer that participates in the PIN Verification Service (PVS), the issuer can choose to have V.I.P. verify PINs on behalf of the issuer center at all times or only when the center is unavailable.

NOTE

PINs are translated in PIN change or unblock requests, but PIN verification is not performed. PIN change and unblock requests are valid for U.K.-domestic transactions only.

The Visa Security Module (VSM) verifies PIN validity using Visa PIN Verification Values (PVVs) or issuer-supplied IBM PIN offsets. BASE I 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, V.I.P. forwards the request to STIP for a decline or pick-up response, depending on issuer specifications.

NOTE

All U.S. issuers are required to test with Visa and verify that they are capable of validating and authorizing PIN-authenticated Visa Debit transactions and are able to support cashback processing.

NOTE

U.S. Visa consumer and commercial prepaid issuers must test with Visa to verify that they are capable of validating and authorizing PIN-authenticated POS transactions, including support of cashback processing, preauthorizations, and preauthorization completion messages.

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 **83** (unable to verify PIN).

Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, of this manual for information about the activity file and about the Cardholder Database. Refer to *V.I.P. System Services, Volume 2*, for a full description of PVS. Refer to the *Payment Technology Standards Manual* for specific technical specifications for PIN translation and verification.

3.7.7 VSDC Service Card and Issuer Authentication Features

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 Data Encryption Standard (DES) key that is loaded on the card during personalization or is produced during a dynamic key-generation session. For card authentication, cryptogram versions 2, 10, 17, and 18 are valid for Visa Integrated Circuit Card Specification (VIS) card types. Cryptogram version 12, and versions 50 to 59 are issuer-proprietary cryptograms. If VisaNet performs the authentication on the issuer's behalf, it forwards the result to the issuer in the request. For Full Data issuers, V.I.P. also incudes the chip card authentication reliability indicator in field 60.7 and audit trail data. Refer to the VSDC Service description in *V.I.P. System Services, Volume 1*, for further information about which conditions must be met for V.I.P. to perform the authentication.

The *Issuer Authentication feature* verifies that the response message came from the correct issuer. If the issuer supports the feature, either VisaNet 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 V.I.P. processing of chip transactions, refer to the VSDC Service description in *V.I.P. System Services, Volume 1* and to the latest version of the *VSDC System Technical Manual* (doc ID 6001–05). Members can contact their Visa representatives to obtain a copy of this manual.

3.8 ASSURED TRANSACTION RESPONSE (ATR) TRACKING

The V.I.P. Assured Transaction Response (ATR) function monitors all authorization requests V.I.P. forwards to issuers to ensure that each request receives a timely authorization response. ATR applies to both BASE I and SMS processing. Refer to the *Visa International Operating Regulations (VIOR)* for issuer response time requirements.

When V.I.P. routes a request to the issuer, it sets a timer to monitor how long the issuer takes to respond. If an issuer does not send an authorization response to V.I.P. within the specified time limit, V.I.P. may invoke STIP to determine the approval or decline decision on the issuer's behalf. If an issuer sends a response after V.I.P. has diverted the corresponding request to STIP, the STIP-generated decision prevails, and V.I.P. discards the response from the issuer.

3.8.1 Member-Level Timeout Settings

ATR functions are controlled by several V.I.P. member profile settings. Issuers should work with their Visa representatives to ensure that their settings result in response times that meet the requirements specified in the *Visa International Operating Regulations*.

3.9 HOW V.I.P. PROCESSES 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 instance, 0101. For purposes of this description, the terms *repeat* and *duplicate* are interchangeable.

IMPORTANT

VisaNet does not allow repeat (duplicate) request messages for ATM transactions. It also does not allow them for any SMS POS or ATM transaction.

V.I.P. considers an authorization request to be a duplicate if the ITT field values (in fields 32, 37, 41, 42, and 63.1) are the same both in the original submission and in the repeated submission. Fields 11, 62.6, and 90 are also key message matching elements. BASE I discards a duplicate message if the original is still being processed, 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 ITT key fields from the original request, BASE I discards the issuer's response. STIP then processes the transaction according to ATR rules if they apply.

If, after receiving an authorization, balance inquiry, or reversal message, the acquirer submits a request (identical to the original) *to the same VIC within 10 seconds of the original*, BASE I treats the second one as a duplicate and returns response code **94** (duplicate transaction). A transaction was submitted that contains values in the tracing data fields that duplicate the values in a previously submitted transaction.) in the response message to the acquirer.

If the acquirer submits a duplicate to the same VIC *after* 10 seconds have passed, BASE I processes the duplicate as a new transaction, that is, STIP or the issuer treats it as a new request.

NOTE

If a request has timed out, acquirers should initiate an 0101 repeat message after waiting a total of 60 seconds. Sixty seconds is the default ATR time-out. Also, if acquirers receive an 0110 response after they have timed out the corresponding request, they should use an 0400 reversal request to ensure that the transaction is properly voided.

If the VIC receives a response from the issuer processor while STIP is already processing the request, or if STIP has already responded on the issuer's behalf, BASE I logs the issuer's late response and discards it with Reason Code **030**—Unsolicited Response Message.

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, V.I.P. converts 0401 messages from BASE I acquirers to 0420 messages before forwarding them to SMS issuers.
- For ATM transactions, a reversal followed by a new request. (VisaNet 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, V.I.P. converts 0101 repeat messages from BASE I 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, V.I.P. converts 0101 repeat messages from BASE I acquirers to 0200 messages and converts 0401 messages to 0420 messages before forwarding them to SMS issuers.

NOTE

BASE I acquirers can identify duplicate responses received from SMS issuers by checking the value in Field 38—Authorization Identification Response. This value is the same in the original response and in the duplicate response.

IMPORTANT

SMS issuers can potentially receive repeat messages. If BASE I acquirers send an 0101 POS request message 10 seconds after the original message has been processed, SMS issuers receive an 0101 request message.

NOTE

Acquirers should ensure that their merchants know to re-swipe the cardholder's card when resubmitting an authorization request after the previous request has been reversed.

Visa recommends limiting repeat message submissions to three per request.

Refer to "Handling Undeliverable Messages" in Chapter 2, BASE I Messages and Flows, for information about how V.I.P. processes undeliverable requests.

3.9.1 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 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 Inter-Task Table (ITT). The ITT empties key field information for a transaction when the response to that transaction has been sent by the issuer or by STIP.

Merchants must ensure that, for field 37:

- Positions 1–4 contain the same date as the one in Field 7—Transmission Date and Time in *YDDD* format.
- Positions 5–6 contain the hours from field 7.
- Positions 7–12 contain the value from Field 11—System Trace Audit Number.

IMPORTANT

*Merchants must not reuse the same value in the last six positions of field 37 in another transaction for at least 60 minutes. Otherwise, BASE I rejects the message with reject code **601**.*

3.9.2 Discard Message Reason Codes

Discarded messages are those V.I.P. identifies as not requiring further processing. When the V.I.P. System determines that a message is to be discarded, it terminates all processing for that message and assigns a reason code.

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 4

BASE I Limits and Routing

4.1 FOREWORD

The following factors determine which transactions V.I.P. sends to stand-in processing (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).

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

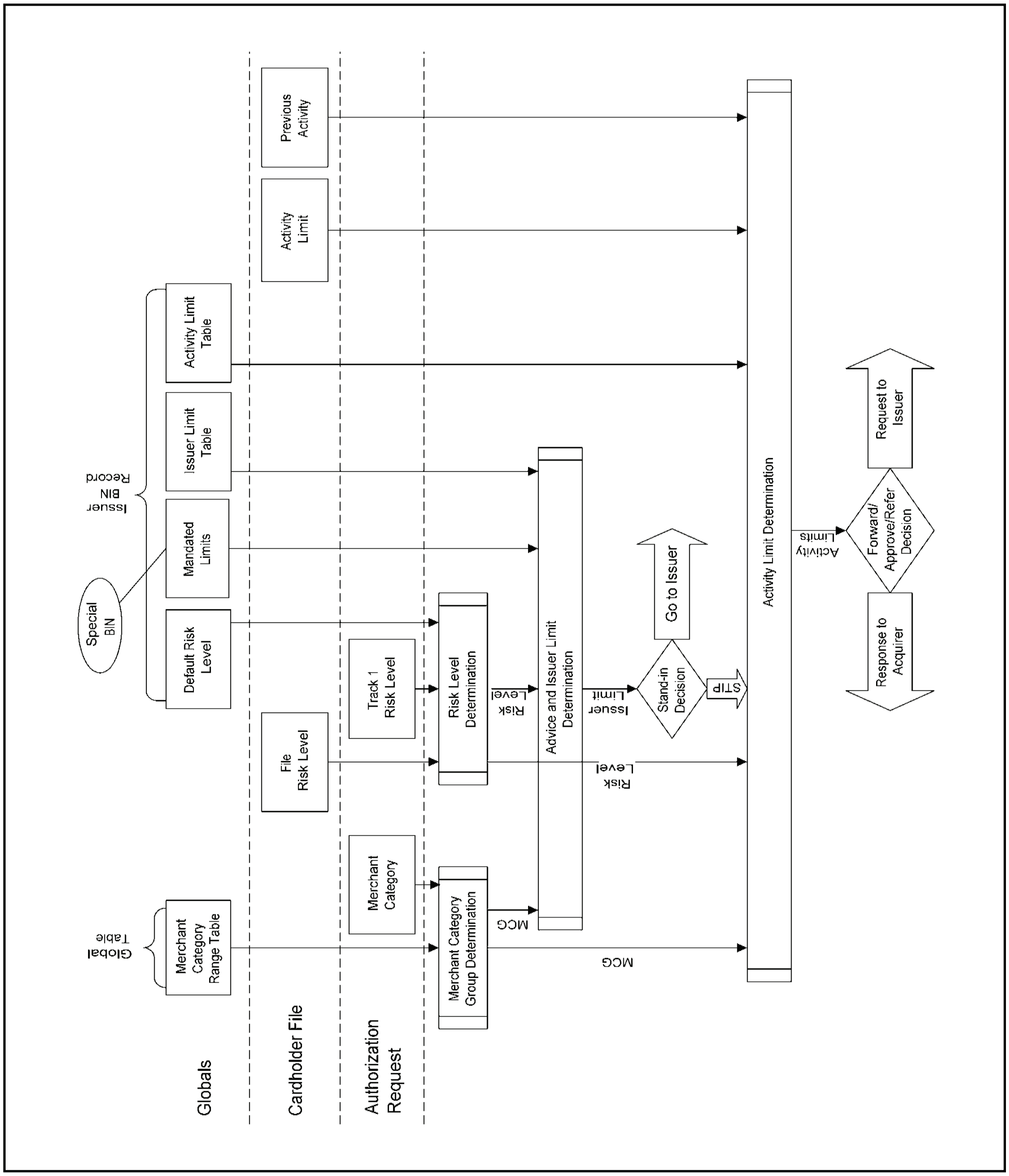
- Selecting risk-level limits and account-level activity limits and determining account listing status, such as **VIP**.
- Applying advice limits if appropriate
- Applying between-limits activity checking if appropriate
- Applying random selection factors if appropriate

NOTE

The V.I.P. System does not apply mandatory minimum issuer or activity limits to debit or prepaid card transactions.

Figure 4-1 illustrates the switching and STIP processes and the relationship among their applicable elements.

Figure 4-1 Switch and STIP Processing Elements



NOTE

Issuer participation in STIP is mandatory; there is no STIP participation option in the Customer Online Repository (CORE), where members processing option selections reside. If the issuer is unavailable for a transaction, STIP processes it and responds to the transaction with the most severe response code. Issuers must participate in Assured Transaction Response (ATR).

4.2 LIMITS OVERVIEW

Limits are thresholds established by the issuer or by Visa. BASE I examines every authorization transaction and uses limits to determine whether to route the transaction to STIP or to the issuer. BASE I 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 their Visa representatives. The limits and their values, along with other processing parameters, are stored in the V.I.P. system tables.

NOTE

Amounts used in BASE I and STIP processing are expressed in U.S. dollars.

Issuer Limit

An *issuer limit* is a dollar amount that determines whether BASE I routes a transaction to the issuer processor or to STIP for an approval, decline, or referral decision. Table 4-1 summarizes how V.I.P. applies issuer-specified or Visa-mandated issuer limits.

Table 4-1 Issuer Limit Processing Decision Summary

Issuer Limit Decision			
Transaction Type	**Use the higher dollar amount of the issuer limit or Visa mandatory minimum limit**	**Use the lower dollar amount of the issuer limit or Visa mandatory minimum limit**	**Exception**
T&E, which includes Travel, Lodging, Auto Rental, Restaurant (if the region defines Restaurant as a T&E transaction)	Yes	No	n/a
MOTO & E-Commerce	No	Yes	Based on member profile parameter, V.I.P. can bypass PCAS and PACM and route all international transactions directly to the issuer.
Purchase & Cash	Yes	No	n/a

Activity Limit

An *activity limit* is the combination of a transaction dollar amount plus the number of times a card can be used during a given period. Table 4-2 summarizes how STIP applies issuer-specified or Visa-mandated activity limits.

Table 4-2 Activity Limit Processing Decision Summary

	Activity Limits Decision		
Transaction Type	**Use the higher dollar amount of the issuer-specified activity limit or Visa mandatory minimum activity limit**	**Use the lower dollar amount of the issuer-specified activity limit or Visa mandatory minimum activity limit**	**Exception**
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 & Cash	Yes	No	

Mandatory Minimum (MM) Limit

For some transactions, the V.I.P. System 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.

V.I.P. System Routing Functions

BASE I processing uses the Positive Cardholder Authorization Service (PCAS) and the Positive Authorization Capacity Management (PACM) Service to establish limits to use for routing and STIP. BASE I uses:

- PCAS-established limits, such as issuer, advice, and activity limits, to route transactions to the issuer or to STIP using issuer limit dollar amounts.
- PACM-established limits to route transactions to the issuer or to STIP primarily using an issuer limit as well as a dynamic limit called the *diversion threshold*. STIP determines this limit by comparing transaction volume to issuer capacity.

4.3 MERCHANT CATEGORY GROUPS

Merchant category groups (MCGs) are collections of similar merchant types that issuers use to specify processing parameters.

BASE I 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 instance, until date, when an issuer chose to block online gambling transactions, VisaNet blocked transactions from MCC 7995. However, now gambling merchants can choose to register with Visa and acquire an MVV to override this block. BASE I directs any transaction originating from a gambling merchant with a valid MVV to the issuer for processing.

See the latest edition of the *Visa International Operating Regulations* for a complete list of Visa-supported MCCs.

NOTE

*V.I.P. does not allow online gambling OCTs destined to recipient issuers in countries where online gambling is prohibited by law. V.I.P. declines the transaction with response code **93** (transaction cannot be completed—violation of law).*

MCGs are grouped into two categories: *Purchases* and *Cash*. The Purchases category, also known as *Non-Cash*, consists of two subgroups: *T&E* and *Purchases*. Table 4-3 shows the transaction categories, transaction types, and their indicators and names.

Table 4-3 Merchant Category Groups

Transaction Category	Transaction Type	MCG Indicator	Merchant Category Group (MCG) Name
Total Purchases	Travel & Entertainment (T&E)	1	Commercial Travel (Airline)
		2	Lodging
		3	Auto Rental
		4	Restaurant
	Purchases (Non-T&E)	5	Mail Order/Telephone Order/e-Commerce (MOTO/EC)
		6	Risky Purchase
		7	Other Purchase
		11	Medical
Total Cash	Cash	8	Other Cash
		9	ATM
		10	Quasi-Cash

BASE I manages MCGs and stores them in the BASE I system tables. Once it identifies the MCG, BASE I 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 V.I.P. Table 4-4 lists the internal MCG indicators.

Table 4-4 MCG Index

MCG Index	
Name	**V.I.P. Index**
Commercial Travel (Airline)	1

Table 4-4 MCG Index (continued)

MCG Index	
Name	**V.I.P. Index**
Lodging	2
Auto Rental	3
Restaurant	4
Mail Order/Telephone Order/e-Commerce (MOTO/EC)	5
Risky Purchase	6
Other Purchase	7
Other (Manual) Cash	8
ATM	9
Quasi-Cash	10
Medical	11

4.3.1 MCG Determination

Key Message Fields for Determining Merchant Category Groups

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

- Field 3—Processing Code, which indicates the transaction type, for instance, a POS purchase transaction or a cash withdrawal.
- Field 18—Merchant Type, a required field in all authorization and reversal requests that contains the code describing the merchant's type of business product or service.
  - If a transaction does not include field 18, BASE I sets the MCG to Other Purchase.
  - If the field 3 processing code indicates Account Funding (**10**), BASE I sets the MCG to Quasi-Cash. BASE I also uses the Quasi-Cash MCG for existing debt transactions and for online (Internet) gambling.
  - For secure e-commerce transactions (field 25 contains **59**), BASE I sets the MCG to MOTO.
  - If the issuer is non-U.S. and field 18 contains **4411** (Cruise Line) or **4112** (Passenger Railway), BASE I sets the MCG to Other Purchase (**07**).
- Field 25—Point-of-Service Condition Code 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/EC authorization request. In some cases, BASE I converts the code supplied by the acquirer. For instance, for e-commerce transactions, BASE I converts code **59**, which signifies e-commerce, to **08** for issuers that not testing for Visa Secure Electronic Commerce (VSEC) programs.
- Field 52—Personal Identification Number (PIN) Data, which, if present in a request, contains an encrypted cardholder PIN or password. ATM cash disbursements, ATM balance inquiry requests, and United Kingdom (U.K.)-domestic PIN change or unblock requests always require field 52. Visa U.S.A. (U.S.)-region-only BASE I POS stand-alone or purchase authorization balance inquiries do not require a PIN.)

Table 4-5 lists the exceptions to determining MCGs.

Table 4-5 Exceptions to Determining MCGs

If...	The MCG Is Set to...
Field 18 is not present	Other Purchase
Field 3 contains **10** (Account Funding), or if the transaction is for an existing debt	Quasi-Cash
If F3.1 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
Field 18 contains **4411** (Cruise Line) or **4112** (Passenger Railway) and the issuer is non-U.S.	Other Purchase

4.4 ISSUER LIMITS

An *issuer limit* is a dollar amount that determines whether STIP or the issuer is to process a transaction.

BASE I routes transactions with amounts equal to or greater than the issuer limit to issuer processors for authorization decisions. BASE I 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.

4.4.1 Zero Issuer Limits

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

- Issuer-unavailable conditions
- Timed-out requests
- Issuer-available conditions such as MOTO

4.4.2 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, BASE I 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, BASE I resets the issuer limit to zero.

4.4.3 Mandatory Minimum Issuer Limits

Regions determine whether their issuers must use MM issuer limits.

For some Visa card transactions, the V.I.P. System overrides an issuer-specified issuer limit with Visa mandatory minimum (MM) issuer limits to facilitate a higher level of cardholder and merchant service. Both PCAS and PACM use the same set of MM issuer limits.

MM issuer limits apply to the following transactions:

T&E—The issuer can also specify limits for these transactions, and BASE I uses the *greater* of the two limits.

e-Commerce—BASE I uses the lower of the mandated or issuer-specified issuer limit. BASE I forces the advice limit to **zero**.

MOTO—BASE I routes transactions below that threshold amount to STIP for the approval or decline decision. U.S.-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, V.I.P. 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, V.I.P. uses the lower of the issuer-supplied issuer limit and the applicable Visa MM issuer limit. For all other purchase or cash disbursement transactions, V.I.P. uses the greater of any issuer-supplied issuer limit and the applicable Visa MM issuer limit.

(Refer to Appendix A, Visa Mandatory Minimum Limits, for the Visa MM issuer limits.)

4.4.3.1 U.S. Minimum Issuer Limit Exemption

U.S. issuers have the option of overriding U.S.-domestic MM issuer limits. The BINs are exempt from international MM issuer limits as well.

NOTE

The Country-to-Country Embargo table must not exclude the use of mandated limits to select a mandated BIN. The Country-to-Country Embargo table is described in detail later in this chapter.

4.5 ADVICE LIMITS

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 issuer processing center is available and for when it is unavailable.

Advice limits control whether or not BASE I 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.

4.5.1 Advice Limit Exception Rules

BASE I changes the advice limit to **zero** if the issuer BIN indicates that BASE I is to force-route all MOTO/EC transactions to the issuer.

The advice limit is **zero** if the region has mandated a **zero** issuer limit for MOTO/EC transactions.

4.6 ACTIVITY LIMITS

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**
>
> *BASE I 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 **255**.
- 1-day amount—The maximum amount allowed for transactions in one day. The one-day amount can be any U.S. dollar amount between **zero** and USD$65,535.00.

Activity limit default values are **255** (count) and USD$65,535.00 (amount). For T&E transactions, using the default values prevents BASE I from checking activity. Also, for T&E transactions, any applicable mandatory minimum limits take precedence over default values, and BASE I checks activity.

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

Table 4-6 shows the relationships of the issuer-available and issuer-unavailable activity limits at the BIN level.

Table 4-6 Issuer Specification Requirements for BIN-Level Issuer and Activity Limits

MCG Category Number	MCG Name	Issuer Available			Issuer Unavailable		Pass Either, Pass Both, or Pass Total *(See notes after table.)*
			Activity Limits		Activity Limits		
		Issuer Limit	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[2]	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

Table 4-6 Issuer Specification Requirements for BIN-Level Issuer and Activity Limits (continued)

MCG Category Number	MCG Name	Issuer Available			Issuer Unavailable		Pass Either, Pass Both, or Pass Total *(See notes after table.)*
			Activity Limits		Activity Limits		
		Issuer Limit	1–Day Amount	1–Day Count	1–Day Amount	1–Day Count	
8	Total Cash	n/a	Required	Required	Required	Required	n/a

1. n/a—These limits cannot be specified.
2. If the ATM Cash sub-limit is greater than the Total Cash limit then the transaction must pass only the ATM Cash sub-limit. If the Total Cash limit is greater than the ATM Cash limit then the transaction must pass both ATM Cash sub-limit and Total Cash limit. Activity limit for ATM Cash is an exception to the Pass Both rule as the sub-limit activity pass is sufficient to pass the activity for an ATM transaction.

Notes on Issuer Specification Requirements for BIN-Level Issuer and Activity Limits Table

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 in CORE. 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 in CORE. 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. (Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for information about the Cardholder Database.)
- Separate activity limits for each cardholder risk level in the BIN.

Regions can specify activity limits for product types and for transaction jurisdictions.

BASE I 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.

4.6.1 Visa Minimum T&E Activity Limits

Visa has established mandatory minimum (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, BASE I 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.

4.6.2 Visa Minimum Non-T&E Activity Limits

BASE I uses the greater of the issuer-specified activity limits or the applicable MM activity limit. Refer to Appendix A, 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 V.I.P. uses the issuer-specified activity limit.

4.6.3 Choosing Issuer-Specified or Visa-Mandated Limits for Routing and STIP

V.I.P. routes a transaction to the issuer or to STIP according to whether the amount in field 4 exceeds the issuer-specified issuer limit threshold amount or, if applicable, the Visa-specified mandatory minimum (MM) issuer limit. To determine which of these limits applies, V.I.P. follows the procedure outlined in Table 4-7. 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 dollar amount is greater (or larger) than the other (less or lower).

Table 4-7 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

BASE I Limits and Routing

Table 4-7 Choosing Issuer-Specified or Visa-Mandated Limits (continued)

To determine the following limit...	For this transaction type	Issuer-specified issuer limit	Visa mandatory minimum issuer limit	Use the following limit
Activity limit	All transactions	Lower	Higher	Visa mandatory minimum activity limit
		Higher	Lower	Issuer-specified activity limit

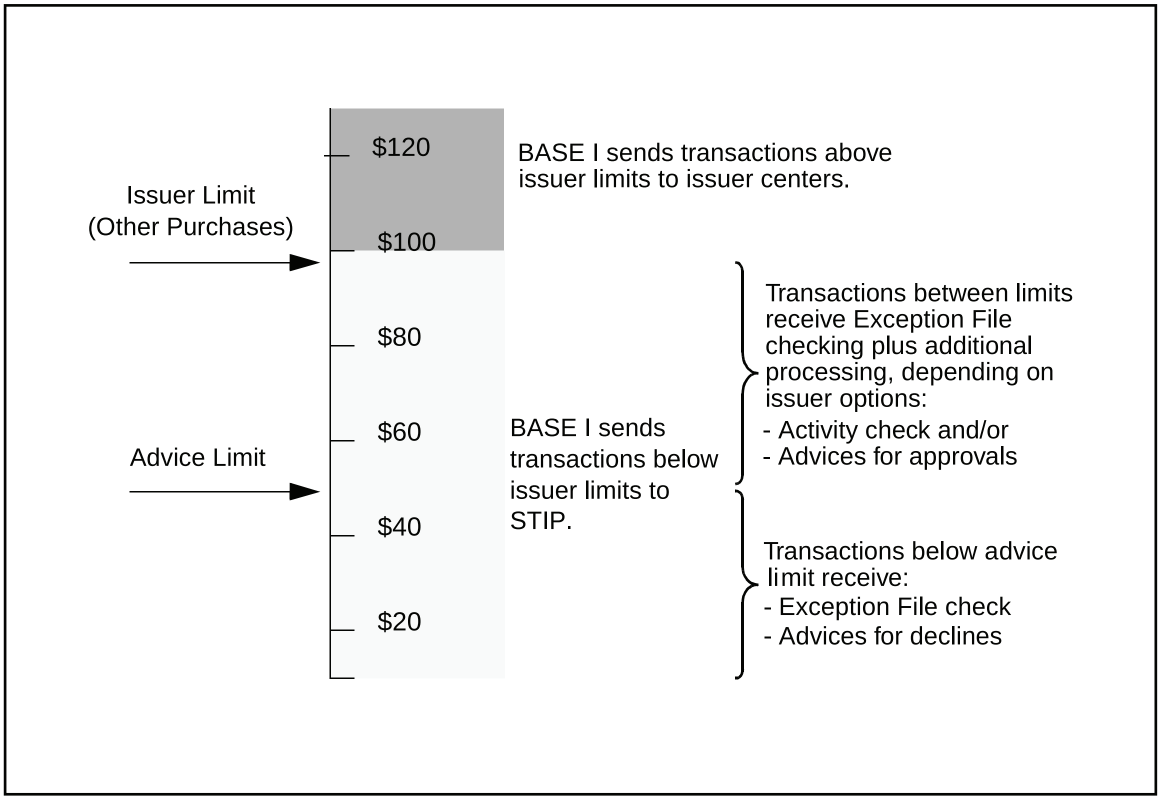
4.7 TRANSACTION CATEGORIES

V.I.P. groups every BASE I authorization into the following three transaction categories:

- Below-advice-limit STIP transactions, that is, the transaction amount is less than the advice limit. For these transactions, BASE I does not perform activity checking or create advices for approved transactions.
- Between-limit STIP transactions, that is, the transaction amount is equal to or greater than the advice limit and less than the issuer limit. BASE I performs activity checking, advice creation, or both, according to issuer options.
- Above-issuer-limit transactions, that is, the transaction amount is equal to or greater than the issuer limit. VisaNet always routes these transactions to the issuer.

STIP processes below-advice-limit and between-limit transactions according to other PCAS rules. Figure 4-2 shows the relationship between these limits.

Figure 4-2 Processing With Different Issuer and Advice Limits


$120
$100
$80
$60
$40
$20
Issuer Limit
(Other Purchases)
Advice Limit
BASE I sends transactions above issuer limits to issuer centers.
BASE I sends transactions below issuer limits to STIP.
Transactions between limits receive Exception File checking plus additional processing, depending on issuer options:
- Activity check and/or
- Advices for approvals
Transactions below advice limit receive:
- Exception File check
- Advices for declines

NOTE

STIP always creates advices for all non-approved PCAS transactions.

Table 4-8 shows how STIP determines whether to create advices for non-approved PCAS and PACM between-limit transactions.

Table 4-8 Advice Creation for Non-Approved PCAS and PACM 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.

Table 4-8 Advice Creation for Non-Approved PCAS and PACM Between-Limit Transactions (continued)

CORE Setting	STIP Decision
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 and all PACM transactions.

4.8 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%**), 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. V.I.P. 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.

4.9 DEFAULT RESPONSE CODES

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, BASE I 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:

- **57**—Transaction not permitted to cardholder.
- **00**—Successful approval or completion.
- **01**—Refer to card issuer.
- **04**—Pick up card.
- **05**—Do not honor.
- **62**—Restricted card.
- **83**—Unable to verify PIN.
- **91**—Issuer unavailable or switch inoperative. (STIP is not applicable or available for this transaction.) Issuers can respond with this code, which BASE I passes to the acquirer without invoking STIP. Issuer processors use this code to indicate that they cannot perform authorization on behalf of the issuer. The code causes a decline at the point of service.

If the response code is **57**, BASE I declines the transaction in STIP and does not create an advice.

4.10 BIN BLOCKING

Issuers can completely block an issuer BIN by setting the default response code to **57** for all MCGs. 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, BASE I declines them with response code **57**.

NOTE

BIN blocking is subject to applicable local law and the international and regional operating regulations governing the issuer's business operations. For all operating regulations, refer to the Visa International Operating Regulations*.*

4.10.1 Country Restrictions

Issuers can specify, at the BIN level, whether cardholders can use their cards:

- In 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 V.I.P. does not permit the transaction, it declines it with response code **62** (restricted card).

4.10.2 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. They also bypass PACM diversion.

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

The available risky country response codes are **A** (approval), **D** (decline), and **R** (referral). V.I.P. translates these codes to **00**, **05**, and **01**, respectively, before it forwards the response to the acquirer.

V.I.P. 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, V.I.P. responds with response code **62** (restricted card) depending on issuer specifications.*

4.10.3 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 before issuing a cardholder certificate. The Certificate Authority, for instance, VeriSign, issues and controls cardholder certificates.

4.10.4 Country-to-Country Embargo

BASE I allows issuers to block transactions originating in or between embargoed countries, for instance, between acquirers in country A and issuers in country B. V.I.P. maintains a Country-To-Country table that allows BASE I 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 BASE I 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 transaction 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.” (Refer to Chapter 5, Stand-In Processing [STIP], for information about the $150 rule.)

When checking the table, BASE I determines if a country is embargoed and if it is, whether the embargo includes cash transactions, POS transactions, or both. When BASE I 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). BASE I controls country-to-country embargoes.

4.11 STIP OR SWITCH DECISION

BASE I routes below-issuer-limit transactions to STIP.

4.11.1 Exception Rules for the STIP or Switch Decision

Table 4-9 lists STIP or switch decisions by transaction type.

Table 4-9 STIP/Switch Decision Rules

Transaction Type or Condition	Always Switch to Available Issuers	Processed in STIP	Comments
Transactions with amounts below the advice limit		✓	n/a
Transactions with amounts above the issuer limit	✓		n/a
Transactions with PINs, CVVs, iCVVs, or CAVVs:			n/a

Table 4-9 STIP/Switch Decision Rules (continued)

Transaction Type or Condition	Always Switch to Available Issuers	Processed in STIP	Comments
• Issuer performs PIN, CVV, iCVV, or CAVV verification	✓		n/a
• VisaNet performs PIN, CVV, iCVV, or CAVV verification		✓	n/a
Mail order or telephone order (MOTO)	✓		BASE I always switches MOTO transactions to available issuers in the U.S. region.
ATM balance inquiry	✓		Ineligible for STIP.
Automated dispensing machine (ADM)	✓		n/a
Transactions involving risky countries	✓		The Risky Countries table indicates force-to-issuer. **NOTE:** *V.I.P. 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**)	✓		n/a
One unit of currency	✓		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 check acceptance transactions and private-label transactions	✓		n/a
United Kingdom (U.K.) Address Verification Service (AVS)-only authorization transactions		✓	When V.I.P. receives an AVS-only account verification request destined for a U.K. issuer that is directly connected to Visa Europe Authorisation Services, V.I.P. forwards the request to Visa Europe Authorisation Services, which determines whether the request is to be processed by its stand-in processing system or forwarded to the issuer.
Address Verification Service (AVS) purchase transactions destined for United Kingdom (U.K.) issuers	✓		All purchase transactions with AVS data (field 123) destined for U.K. issuers.

Table 4-9 STIP/Switch Decision Rules (continued)

Transaction Type or Condition	Always Switch to Available Issuers	Processed in STIP	Comments
Certain Visa Electron transactions			If a PIN is present, the transaction is not ATM (field 18 does not contain **6011**), V.I.P. is not verifying the PIN, and any of the following options are ***not*** set to On: • Decline all non-domestic transactions. • Decline POS transactions with PINs in STIP. • Decline all POS transactions with PINs. If the issuer BIN has any of the following Visa Electron options selected: • Decline card-not-present transactions in STIP. • Decline POS transactions with PINs in STIP. • Decline POS transactions without PINs in STIP.
Recurring payment transactions	✓		If the issuer is unavailable, STIP processes the transaction according to issuer parameters.
Bill payment transactions	✓		If the issuer is unavailable, STIP processes the transaction according to issuer parameters.
PIN change or unblock transactions (Visa Smart Debit/Smart Credit [VSDC] PIN Management Service; U.K.-domestic transactions only)	✓		If the issuer is unavailable or times out, STIP responds with code **91**.
POS balance inquiry (stand-alone)	✓		Ineligible for STIP. **NOTE:** *This is a U.S. region-only service.*
POS balance inquiry as part of a purchase authorization request		✓	If the issuer is unavailable or times out, STIP responds according to issuer STIP parameters as if the balance inquiry were not involved. **NOTE:** *This is a U.S. region-only service.*
V PAY	✓		

Table 4-9 STIP/Switch Decision Rules (continued)

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	✓		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. 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. If issuer is unavailable, STIP uses issuer-specified parameters and issuer-specified response to acquirer.

If issuers respond to a BASE I authorization request with code **NO** in field 39 (force to STIP) in the 0110 response, V.I.P. 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.

4.12 PACM DECISION

The Positive Authorization Capacity Management (PACM) Service includes issuer traffic flow in the STIP or switch equation. The service monitors the flow rate (volume) of PACM-eligible messages to the participating issuer's processor and compares the rate to the issuer processing center's capacity information. PACM uses this volume-to-capacity ratio to determine the optimum percentage of eligible authorization requests that BASE I should divert to STIP. This percentage is associated with a diversion level that has an assigned transaction amount, or *diversion threshold*. PACM uses this diversion threshold to determine which transactions to send to the issuer and which transactions to send to STIP. BASE I sends transactions above this amount to the issuer processor. The system sends transactions at or below this amount to STIP.

The PACM diversion-level dollar-amount thresholds are somewhat different from Positive Cardholder Authorization Service (PCAS) issuer limits:

- PACM amount thresholds are related to issuer processing center capacity, the volume of transactions, and the transaction amounts.
- PCAS issuer limits are related only to transaction amounts.
- Visa establishes PACM diversion threshold amounts.
- Issuers establish issuer limits (with the exception of mandated limits established by Visa).

To make the diversion decision, PACM first determines whether the transaction is eligible for diversion. Second, PACM determines if the transaction amount is below the diversion threshold.

BASE I Limits and Routing

4.12.1 Diversion Eligibility

PACM determines eligibility for diversion in three ways:

- PACM always diverts certain transactions to STIP, regardless of issuer capacity.
- PACM considers certain transactions eligible for diversion to STIP.
- PACM never diverts certain transactions to STIP, regardless of issuer capacity.

4.12.1.1 Transactions Always Diverted to STIP

For PACM Service participants, BASE I always routes the following transactions to STIP:

- Telecode verifications.
- Authorization requests with transaction amounts under the Visa T&E mandatory minimum issuer limits for the MCG of the transaction. If the transaction is governed by Visa MM issuer limits for T&E transactions, BASE I uses the issuer limits to route PACM-controlled transactions to STIP even if the transaction amount is below the diversion threshold and the issuer processing center's capacity has not been exceeded.

The next section identifies transactions that could be eligible for PACM diversion, depending on issuer specifications.

4.12.1.2 Transactions Eligible for PACM Diversion

PACM considers the following transactions eligible for diversion to STIP:

- Purchases, purchases with cashback
- Recurring payment
- Bill payment
- Restaurant
- Medical
- T&E transactions over, or exempt from, the applicable Visa MM issuer limits

The following section identifies transactions that PACM never diverts to STIP regardless of whether the issuer participates in the PACM Service.

4.12.1.3 PACM Transactions Never Diverted to STIP

PACM never diverts the following transactions to STIP:

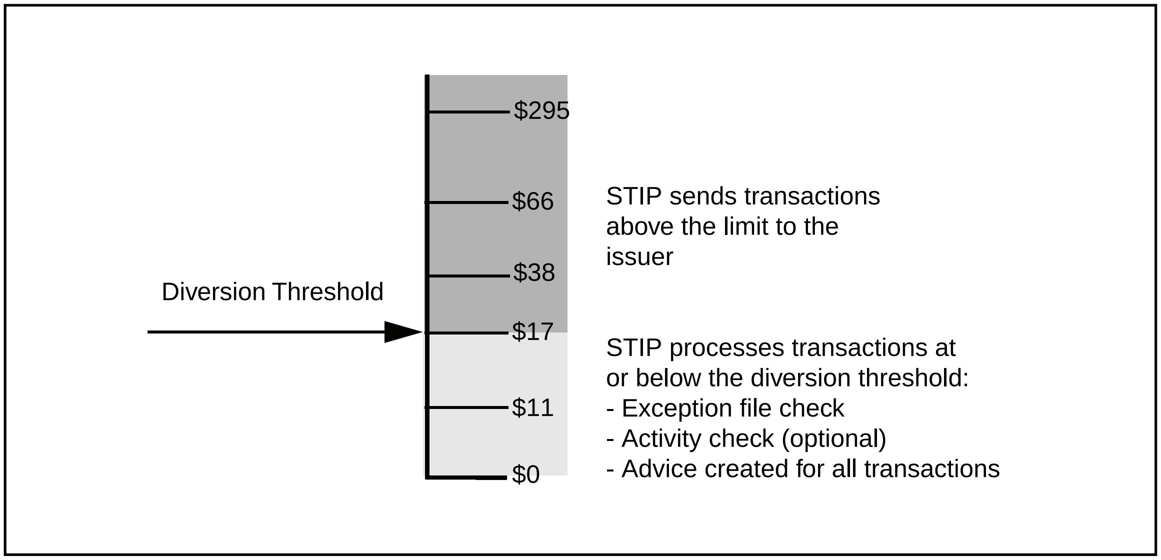
- ATM cash, quasi-cash, and other cash
- Mail order or telephone order (MOTO)
- e-Commerce, including CAVV
- Risky purchase (certain merchant category groups with higher than average fraud rates)
- Risky country
- Status check (single unit of currency authorization) and balance inquiry
- Traffic destined for acquirers
- Issuer traffic for BINs not enrolled in PACM
- Commercial card large-ticket transaction
- PIN change or unblock request

Once PACM determines whether the transaction is eligible or not, the service then determines whether the transaction is within the limits of the diversion threshold.

4.12.2 Diversion Processing

Under PACM, BASE I forwards all eligible transactions to the issuer unless the processor's capacity has been reached. When PACM monitoring detects that per-minute volume exceeds the issuer processor's capacity, PACM routes low-risk transactions to STIP for the next 60 seconds. Figure 4-3 illustrates diversion processing.

Figure 4-3 PACM Diversion Processing


$295
$66
$38
$17
$11
$0
Diversion Threshold
STIP sends transactions above the limit to the issuer
STIP processes transactions at or below the diversion threshold:
- Exception file check
- Activity check (optional)
- Advice created for all transactions

For PACM diversion to take place, PACM must determine the diversion threshold. Determining the diversion threshold entails the following three steps:

1. Determining processor capacity
2. Calculating a diversion level
3. Checking the BASE I diversion tables for the diversion threshold

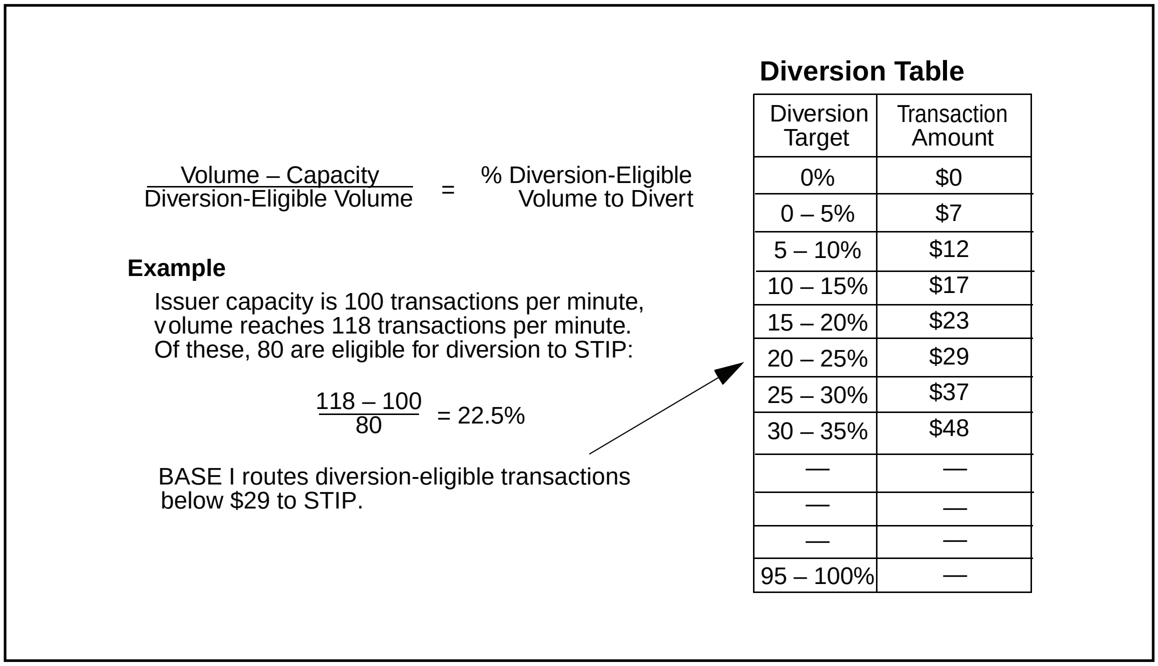
4.12.2.1 Calculating a Diversion Level

Every 60 seconds, PACM checks the transaction volume between the issuer and VisaNet and compares it to the issuer's rated capacity. If the volume for a given minute is greater than 1/60 of the rated hourly capacity, PACM calculates the diversion level and invokes (or continues) transaction diversion for the next 60 seconds.

The diversion level corresponds to the percentage by which transaction volume exceeds the processor's rated capacity. PACM continuously monitors transaction volume and capacity to ensure that it is diverting the optimum transaction volume and is adjusting the diversion level accordingly.

Figure 4-4 illustrates how PACM calculates a diversion level.

Figure 4-4 PACM Calculation of Diversion Level



$$\frac{\text{Volume} - \text{Capacity}}{\text{Diversion-Eligible Volume}} = \text{\% Diversion-Eligible Volume to Divert}$$

Example

Issuer capacity is 100 transactions per minute, volume reaches 118 transactions per minute. Of these, 80 are eligible for diversion to STIP:

$$\frac{118 - 100}{80} = 22.5\%$$

BASE I routes diversion-eligible transactions below $29 to STIP.

Diversion Table

Diversion Target	Transaction Amount
0%	$0
0 – 5%	$7
5 – 10%	$12
10 – 15%	$17
15 – 20%	$23
20 – 25%	$29
25 – 30%	$37
30 – 35%	$48
—	—
—	—
—	—
95 – 100%	—

PACM suspends advice traffic for all BINs connected to a processing center when the total processing center volume exceeds its processing capacity. This precaution preserves issuer processor capacity for real-time authorization decisions. When transaction volume drops below capacity, BASE I resumes advice delivery. PACM includes advice volume in overall processing center volume. Advices created for PACM processing can include optional PACM indicators in Field 44.6—PACM Diversion Level Code and in Field 44.7—PACM Diversion Reason Code.

4.12.2.2 BASE I PACM Diversion Tables

V.I.P. stores diversion levels in multiple PACM diversion tables. BASE I and SMS each has separate PACM diversion tables.

PACM refers exclusively to the applicable diversion table during the initial diversion minute. During each subsequent diversion minute, PACM monitors how close it has come to diverting the targeted volume of transactions. PACM factors in this percentage to select the diversion level for the next 60 seconds. This continuous monitoring reduces the effects of transaction mixtures that differ from the percentages in the diversion table.

For BASE I issuers, each region can define its own diversion tables. Table 4-10 lists the BASE I PACM diversion levels and the default threshold dollar amounts for the six Visa regions:

1 = Visa U.S.A. (U.S.)

2 = Visa Canada (CAN)[1]

3 = Visa Europe (VE)

4 = Asia-Pacific (AP)

5 = Latin American and Caribbean (LAC)

6 = Central Europe, Middle East, and Africa (CEMEA)

[1] The V.I.P. System internally refers to Canada as “CA” and uses CA when referring to actual code; otherwise, the abbreviation for Canada is “CAN” in V.I.P. documentation.

Table 4-10 BASE I PACM Diversion Tables by Visa Region

Diversion Level	Percentage of Eligible Transactions Diverted to STIP	BASE I DIVERSION TABLES Dollar Value of Diverted Transactions (Eligible if Below Listed Amount)		
		Regions 1 (US), 2 (CAN), 5 (LA)	Regions 3 (VE), 6 (CEMEA)	Region 4 (AP)
00	00	0	0	0
01	05	8	14	11
02	10	12	20	14
03	15	14	26	16
04	20	17	31	19
05	25	19	38	22
06	30	22	44	25
07	35	25	52	29
08	40	28	59	33
09	45	31	68	38
10	50	36	76	45
11	55	40	87	54
12	60	46	102	64
13	65	52	118	75
14	70	59	140	89
15	75	70	160	107
16	80	85	188	131
17	85	105	235	160
18	90	151	314	212
19	95	253	403	321
20	100	99,999	99,999	99,999

4.12.3 Key Message Fields

BASE I conveys PACM activity in BASE I 0120 advices using the following fields:

- Field 44.1—Response Source/Reason Code: A value of **2** in this field indicates that PACM handled the transaction, and that the amount was below the sliding dollar amount.
- Field 44.6—PACM Diversion Level: The value in this field indicates which of the 20 diversion levels PACM used at the time it processed the transaction. Each diversion level describes by what percentage volume exceeded the issuer processor's capacity.
- Field 44.7—PACM Diversion Reason Code: The value in this field indicates the reason PACM diverted the transaction to STIP. Currently, the only diversion reason code available is **A** (volume exceeded capacity).

See Chapter 5, Stand-In Processing (STIP), for information about stand-in processing of PACM transactions. Refer to *V.I.P. System Services, Volume 2*, for more information regarding PACM. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for more field information.

4.13 CARDHOLDER RISK LEVELS

Issuers use cardholder risk levels to tailor authorization routing parameters for cardholders within a BIN. BASE I 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 4-11 summarizes the four levels.

Table 4-11 Cardholder Risk Levels

Risk Level	Applies to	Comments
A	Premier or lowest risk accounts	Generous parameters.
B	Lower or higher risk accounts	Parameters established according to issuer preference.
C	Median risk accounts	BASE I 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*. Issuer processing centers can assign one or more of the following limits to each risk level:

- Activity limits by MCG. These include:
  - Count and amount limits.
  - 1-day and 4-day multipliers. (See Chapter 5, Stand-In Processing [STIP], for information about 4-day multipliers.)
  - Issuer-available and issuer-unavailable processing parameters.

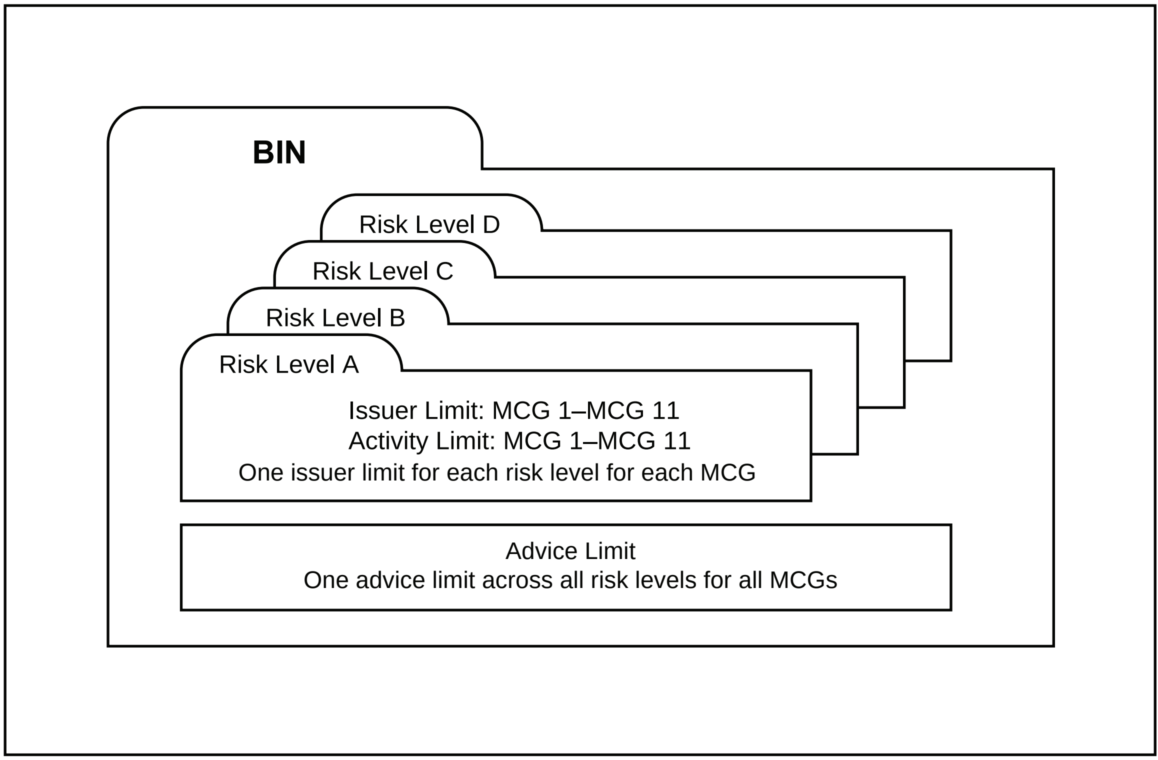
NOTE

Cardholder risk-level activity limits override any BIN-level 1-day dollar 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 4-5 shows the relationship of the issuer limit and the advice limit settings for cardholder risk levels.

Figure 4-5 Issuer and Advice Limit Settings


BIN
Risk Level D
Risk Level C
Risk Level B
Risk Level A
Issuer Limit: MCG 1–MCG 11
Activity Limit: MCG 1–MCG 11
One issuer limit for each risk level for each MCG
Advice Limit
One advice limit across all risk levels for all MCGs

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, BASE I would route all Restaurant authorization requests of USD$200.00 or more to the issuer for processing. STIP would process requests under USD$200.00. For risk level C cardholders, BASE I would route all Restaurant authorization requests of USD$75.00 and above to the issuer for processing. STIP would process requests under USD$75.00.

Issuers can specify risk levels by one of two methods:

- Encoding Track 1 in the magnetic stripe of the card when the issuer issues the card. Visa 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. Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for information about the CDB.

Although BASE I usually does not retrieve the CDB during routing determination, BASE I 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.

Chapter 5

Stand-In Processing (STIP)

BASE I *stand-in processing (STIP)* makes authorization decisions to approve, decline, or refer a transaction on the issuer's behalf.

BASE I 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. If the Processing Center Record (PCR) option for the ATR feature is not on, BASE I always discards messages that time out and does not perform stand-in processing.
- 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 participates in the Positive Authorization Capacity Management (PACM) Service, the issuer's processor capacity is exceeded, and the transaction amount is below the current diversion threshold.
  - The issuer subscribes to certain Visa 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 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.

STIP makes authorization decisions to approve, decline, or refer transactions on behalf of issuers. This chapter summarizes the processing decisions for transactions that have been routed to STIP.

Issuers can set the following preferences separately for domestic and international chip transactions (in which the chip magnetic-stripe is read, or in which no PIN is entered when it is required and a PIN pad is present):

- Route to issuer (yes or no).
- STIP response (approve or decline).

STIP performs the following tasks:

- Performs various exception checks to determine if STIP should decline the transaction.
- Evaluates response codes provided by the issuer.
- Performs miscellaneous edits for check digits and expiration 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.

This chapter describes these tasks in detail.

NOTE

STIP may convert referral response codes it generates to decline response codes based on the transaction type or on regional or issuer options.

5.1 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, V.I.P. terminates STIP processing and immediately generates a response. Table 5-1 lists the conditions under which V.I.P. 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 5-1 Transactions Declined in STIP

Transaction Type	Condition	STIP Response Code
ATM Balance Inquiry	Issuer is unavailable and supports ATM balance inquiry transactions.	Response Code **91**
	Issuer does not support ATM balance inquiry transactions.	Response Code **57**
POS Stand-Alone Balance Inquiry	Issuer is unavailable and supports U.S. POS balance inquiry transactions.	Response Code **91**
	Issuer does not support U.S. POS balance inquiry transactions.	Response Code **57**
Recurring Payment	Expired or missing expiration date.[1]	Response Code **05**
Key-Entered	Issuer has opted to decline all key-entered transactions (field 22 is not present or the value is **01**).	Response Code **05**

Table 5-1 Transactions Declined in STIP (continued)

Transaction Type	Condition	STIP Response Code
Visa Electron	Key-entered non-domestic transaction. POS transactions, card not present. POS transactions with PIN. **NOTE:** *Issuers specify the Decline option for each of these Visa Electron transaction types in the system files (using the Customer Online Repository (CORE).*	Response Code **91**
	POS transactions without PIN. **NOTE:** *Issuers specify the Decline option for this Visa Electron transaction type in the system files (using CORE).*	Response Code **57**
POS With PIN	Issuer has chosen to decline POS transactions with PINs.	Response Code **57**
Visa Credential Server	Status check transactions in which the merchant category code in Field 18—Merchant Type is **9701** (Visa Credential Server).[2]	Response Code **91**
Visa Distribution Card	Issuer unavailable.	Response Code **91**
Large-Ticket (GSA, non-government commercial card above USD$499,999.99)	Issuer unavailable.	Response Code **91**
Large-Ticket (Visa Infinite, Visa Signature, or Visa Signature Preferred above USD$99,999.99)	Issuer unavailable.	Response Code **91**
Mail Order/Telepone Order (MOTO) or Electronic Commerce (e-Commerce) Online Gambling (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.[3]	Response Code **57**

Table 5-1 Transactions Declined in STIP (continued)

Transaction Type	Condition	STIP Response Code
PIN Change or Unblock (VSDC PIN Management Service; United Kingdom (U.K.)-domestic transactions only)	Issuer unavailable.	Response Code **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 expiration 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 expiration date.
2. These transactions must be routed to the issuer so the Certificate Authority can issue cardholder certificates.
3. Members can choose to have STIP decline all MOTO transactions as well as Internet gambling transactions. However, online gambling transactions having valid MVVs are sent to the issuer for processing.

5.2 STIP SETUP

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, for instance, checking expiration dates or the Exception File, or processing for services such as Cardholder Authentication Verification Value (CAVV) Verification Service, Card Verification Value (CVV/iCVV) Service, Dynamic Card Verification Value (dCVV) Service, or PIN Verification Service (PVS). 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.

5.3 EVALUATING RESPONSE CODES PROVIDED BY ISSUER

STIP determines the issuer-specified response codes based on the following considerations:

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

5.3.1 Issuer Available and Unavailable Default Response Codes

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 honor

57—Transaction not permitted to cardholder

83—STIP cannot verify PIN

91—Issuer is unavailable

NOTE

*Issuers can respond with code **91**, which BASE I passes to the acquirer without invoking STIP. Issuer processors use this code to indicate that they cannot perform authorization on behalf of the issuer. The code causes a decline at the point of service.*

5.3.2 Response Codes That Can Override the Default Response Code

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. BASE I controls country-to-country embargoes.

5.3.3 CVV or iCVV Failure Response Code

If V.I.P. 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 U.S. POS balance inquiry and the CVV or iCVV failure response code is an approval, STIP changes the response to a decline (**05**).

5.3.4 CVV2 Failure Response Code

A *Card Verification Value 2 (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 that have successfully completed testing to receive the field. (Visa recommends this testing.)

5.3.5 CAVV Failure Response Code

If V.I.P. performs CAVV validation, and the CAVV validation fails or V.I.P. cannot completed 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 CAVV Verification 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.

V.I.P. accepts Visa authorization and full financial requests submitted with both a CAVV and a CVV2. When V.I.P. 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, V.I.P. validates the CAVV first:

- If the CAVV validation is successful, V.I.P. 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 Service rules apply:
  - If the issuer specifies that V.I.P. is to decline all transactions that fail the CAVV check, V.I.P. declines the transaction without verifying the CVV2.
  - If the issuer specifies that V.I.P. is to forward all results to the issuer regardless of the outcome, V.I.P. 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 V.I.P. processing when both elements are present in a request, refer to the CAVV Verification Service chapter in V.I.P. System Services, Volume 2*.*

5.3.6 PVS Failure Response Code

If the transaction fails PIN Verification Service (PVS) PIN verification, V.I.P. saves response code **55** (incorrect PIN) in the PVS response code field. If the number of allowable invalid PIN-entry attempts is exceeded, V.I.P. saves the interim response code **75** (allowable number of PIN-entry tries exceeded) instead and converts it to code **05**, although it forwards code **75** to the issuer in the 0120 advice. If the issuer returns response code **75** in field 39 of the 0110 response, V.I.P. forwards the field 39 code unchanged to the acquirer; otherwise, V.I.P. inserts response code **05** in field 39 before forwarding the response to the acquirer.

V.I.P. records each incorrect PIN-entry attempt and accumulates the total in the activity file in the Cardholder Database. Refer to the PIN Verification Service (PVS) chapter in *V.I.P. System Services, Volume 2*, for an explanation of V.I.P. processing when the number of unsuccessful PIN-entry attempts exceeds the issuer-set limit.

If the transaction is POS (not ATM or cash) and the issuer has not chosen to have V.I.P. perform PIN verification, STIP sets the PIN verification response code to **83**, or immediately replies to the transaction with response code **57** (transaction not permitted to cardholder) if the issuer has selected this option.

5.3.7 VSDC Response Code

During chip card transaction processing, issuers can select a response code, depending on the error condition encountered. Currently, issuers can specify response codes for 28 different conditions.

See Chapter 1, The BASE I System and the VisaNet Network, for basic information about VSDC processing. Also refer to the Visa Smart Debit/Smart Credit (VSDC) Service chapter in *V.I.P. System Services, Volume 1*, and to the *Visa Smart Debit/Smart Credit System Technical Manual*.

5.3.8 “$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 non-mail order, telephone order, or electronic commerce (MOTO/EC) purchase transactions, STIP responds to the acquirer with an approval or a decline rather than a referral. Issuers can specify different response codes for different risk levels if issuers are using risk levels to classify cardholders. Table 5-2 shows the MCGs eligible for the $150 rule.

Table 5-2 MCGs Eligible for the $150 Rule

MCG	Description	Eligible	Not Eligible
01	Airline	✓	

Table 5-2 MCGs Eligible for the $150 Rule (continued)

MCG	Description	Eligible	Not Eligible
02	Lodging	✓	
03	Auto Rental	✓	
04	Restaurant	✓	
07	Other Purchase	✓	
05	MOTO/EC		✓
06	Risky Purchase		✓
08	Other Cash		✓
09	ATM Cash		✓

The “$150 rule” *does not* apply to:

- Automated dispensing machine (ADM) transactions.
- Risky purchase transactions.
- Visa Electron transactions. V.I.P. generates response code **05** in field 39 if the activity amount or the activity count is exceeded.

The “$150 rule” *does* apply to domestic and international transactions. It is mandatory for U.S. issuers.

5.3.8.1 Suspected Fraud

When SMS issuers respond to 0100 authorization requests from BASE I acquirers, they can use response code **59** in field 39 to alert Visa of suspected fraud. Along with converting the 0210 response message to an 0110 response message, V.I.P. also changes code **59** to code **05** (decline) before forwarding the 0110 response to the acquirer. The usage of code **05** minimizes the possibility of problems between the merchant and the cardholder.

5.4 MISCELLANEOUS EDITS

When applicable, STIP verifies account numbers, expiration 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 V.I.P. 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]).
- Expiration date edits:
  - If the expiration 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 expiration date is invalid, STIP generates response code **54** (expired card) for the response.
  - If the transaction is mail order, telephone order, or e-commerce (MOTO/EC) and the issuer does not allow MOTO/EC transactions without an expiration date in issuer-unavailable situations, STIP generates response code **05** for the response.

  NOTE

  Refer to “Expiration Date Edits” in this chapter 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 **01** (referral) for the response.

Account number, account number length, and expiration date edits do not apply to check acceptance transactions. V.I.P. bypasses the expiration date check for reversals and for Visa Electron transactions.

5.4.1 Mod-10 Account Number Checks

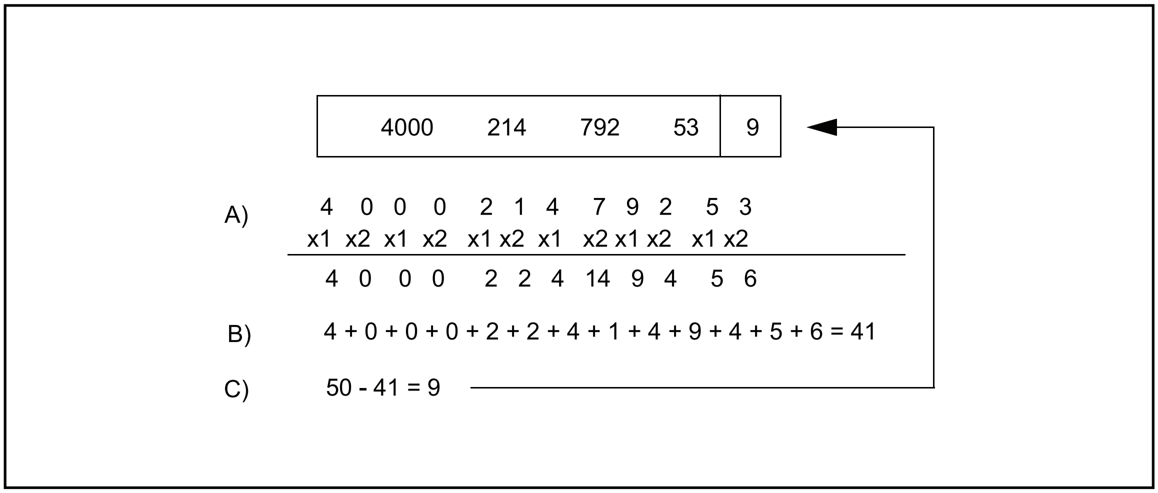
STIP does not perform account number verifications on alphanumeric account numbers (non-standard account numbers) or for account numbers in exception file update messages.

Luhn Modulus-10 Algorithm—BASE I 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, BASE I multiplies every other number by **2**. Starting with the second-to-last number, BASE I multiplies every other number by **1**.
2. BASE I calculates the sum of the digits of the values created in step 1.
3. From the next higher multiple of **10**, BASE I 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 5-1 illustrates the calculation process that BASE I uses to calculate the check digit for a 13-digit account number.

Figure 5-1 Modulus-10 Check Digit Algorithm Calculation Example



5.4.2 Expiration Date Edits

STIP edits expiration dates depending on whether the expiration date is present in the message in Field 14—Date, Expiration, and whether the issuer has established that STIP can process MOTO/EC transactions (Field 25—Point-of-Service Condition Code contains **08**) without expiration dates. Expiration dates must be in a valid *YYMM* numeric format: *YY* = year (**00**–**99**), and *MM* = month (**01**–**12**).

V.I.P. considers a field 14 expiration date to be expired if it is 50 years greater than the current date.

If the expiration date is invalid or has expired, STIP sets the expiration date response code to **54**, and sets the internal indicator to indicate that the transaction should be forward-referred to the issuer, if available. V.I.P. includes the response code in 0110 responses from STIP as well as in STIP advices.

If the expiration date is not present and the transaction meets one of the following qualifications, STIP sets the expiration 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/EC transaction (field 25 does not contain **08**).
- It is a MOTO/EC transaction (field 25 contains **08**) and the issuer has established that it does not want V.I.P. to approve MOTO/EC transactions in STIP that do not have an expiration date.
  - If issuers instruct V.I.P. to process MOTO/EC transactions that lack an expiration date, V.I.P. 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.
- It is not a Visa Electron transaction.

5.4.2.1 Manually Prepared Authorizations Without Expiration Dates

STIP processes manual authorization requests (field 22 contains **01**) that lack expiration dates as follows:

1. V.I.P. declines the request with response code **05** (do not honor) in field 39 if:
   - The issuer processor is unavailable or times out, ***and/or***
   - The transaction is anything but MOTO/EC, or the transaction is MOTO/EC, and the issuer BIN option requires that MOTO/EC transactions include the expiration date.
2. V.I.P. 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/EC, or the transaction is MOTO/EC, and the issuer BIN option requires that MOTO/EC transactions include the expiration date.
3. If the issuer processing center approves the request, the issuer processing center changes the response code in the response message before it returns it to BASE I.

5.5 SERVICE CODE EDITS

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:

- V.I.P. performs service code edits only for Visa and Visa Electron cards.

  NOTE

  Visa allows CVV and CVV2 emergency replacements for Visa Electron cards for all regions ***except*** *the U.S. region (region 1) and the Canada region (region 2).*

- 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*.

5.6 EXCEPTION FILE CHECK

The following conditions apply to Exception File checking:

- The Exception File can contain approval, decline, pick-up, **XA**, **XD**, , 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**, V.I.P. 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 5-3. If there are no activity limits set in the risk limits file, the limits associated with the **A1**–**A9** codes apply. These limits override values specified at the BIN level. BASE I uses the same limits for both subtotal limits and total limits.

Table 5-3 lists activity limits for the special response codes **A1**–**A9**.

Table 5-3 Special Response Code Activity Limits

Exception File Response Code	1-Day Amount	1-Day Count	4-Day Amount	4-Day Count
A1	USD1,500.00	3	USD1,500.00	9
A2	USD2,000.00	5	USD3,500.00	12
A3	USD3,000.00	8	USD6,000.00	14
A4	USD4,500.00	12	USD8,000.00	25
A5	USD6,000.00	15	USD10,000.00	40
A6	USD8,000.00	20	USD14,000.00	50
A7	USD10,000.00	25	USD20,000.00	100
A8	USD1,500.00	4	USD2,000.00	10
A9	USD2,250.00	6	USD3,500.00	13

If the exception file lists the cardholder account number, the value in the action code field determines how STIP processes requests on that account, as specified in Table 5-4.

Table 5-4 Effect of Exception Records on STIP Authorization

Action Code		Action Taken
11	**VIP** Code	V.I.P. checks the issuer-specified amount limit and performs activity checking.
A1–**A9**	Other **VIP** Codes	The code identifies the special high-value activity limit STIP is to use.
05 **04**, **07**, **41**, **43**	Decline Decline and Pick-Up	STIP does not perform activity checking.

Table 5-4 Effect of Exception Records on STIP Authorization (continued)

Action Code		Action Taken
01	Referral	STIP (1) places the code in the request and (2) sends the request to the issuer center. If the center is not available, STIP processing continues.
XA	Forward or Approval	STIP (1) places the code in the request and (2) sends the request to the issuer center. If the center is not available, STIP checks activity as specified by the center and assigns a standard approval (code **00**) to the request.
XD	Forward or Decline	STIP (1) places the code in the request and (2) sends the request to the issuer center. If the center is not available, STIP assigns a standard decline (code **05**) to the request.

Refer to Chapter 6, The Cardholder Database, Merchant Central File, and Advice File, for more exception file information. Refer also to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

5.7 ACTIVITY CHECK

STIP determines activity limits and performs activity checking.

NOTE

*BASE I 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.)*

5.7.1 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.

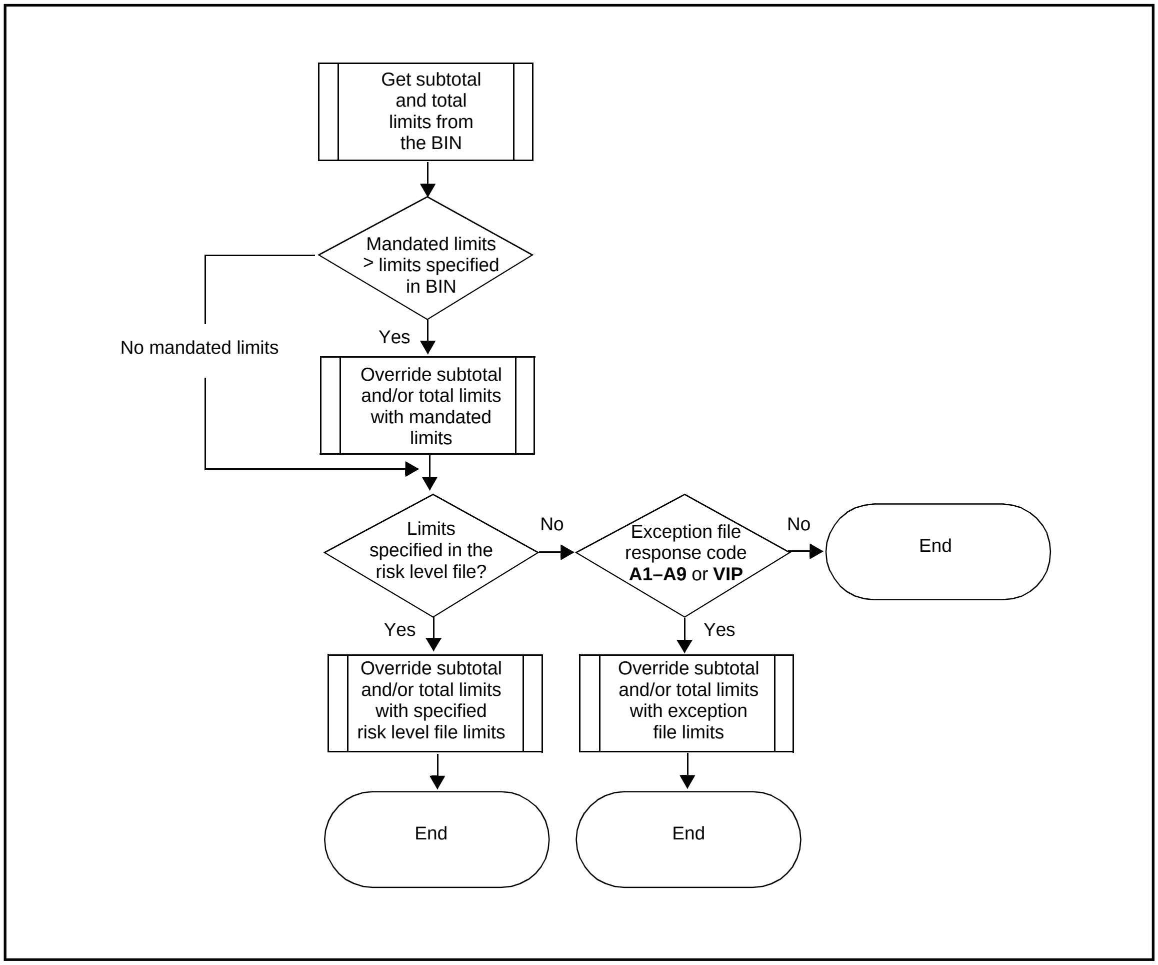
Separate activity limit sets exist for issuer-available and issuer-unavailable conditions. V.I.P. uses issuer-unavailable activity limits when the issuer has signed off, when VisaNet thinks the issuer is offline, or when a transaction sent to the issuer times out.

Figure 5-2 illustrates how V.I.P. determines activity limits.

NOTE

Figure 5-2 illustrates a general flow that shows how STIP determines activity limits. This flow does not show exception scenarios.

Figure 5-2 Activity Limits Determination


Get subtotal and total limits from the BIN
Mandated limits > limits specified in BIN
No mandated limits
Yes
Override subtotal and/or total limits with mandated limits
Limits specified in the risk level file?
No
Exception file response code A1–A9 or VIP
No
End
Yes
Yes
Override subtotal and/or total limits with specified risk level file limits
Override subtotal and/or total limits with exception file limits
End
End

5.7.1.1 Limit Selection Hierarchy

When issuers establish limits at multiple levels, STIP uses the hierarchy in Table 5-5 to determine processing parameters.

Table 5-5 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

Table 5-5 Activity Limit Selection Hierarchy (continued)

These Limits	Supersede the Following:	Under These Circumstances:
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	When MM limits apply and the Visa MM activity limit is higher than the issuer-specified activity limit.
Account-specific limits	MM activity limits	Always
	Non-default risk limits	
	Default risk-level BIN limits	

5.7.2 Testing Activity

STIP tests activity as described below.

- 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.

5.7.2.1 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.) V.I.P. 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, V.I.P. 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, V.I.P. checks the Total Purchase activity limits. If the transaction amount is below these limits, V.I.P. 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.

5.7.2.2 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, BASE I 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, BASE I increments the MCG's count and amount accumulators and approves the transaction. If there are MCG activity limits, the transaction must pass them for BASE I 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, BASE I increments the Total Purchase count and amount accumulators and approves the transaction; otherwise, BASE I 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.

Mail Order/Telephone Order/e-Commerce (MOTO/EC) 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. BASE I updates the MCG-level activity limit and Total Purchase activity limit accumulators as appropriate.

Medical and Other Purchase—BASE I 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 BASE I 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.

5.7.2.3 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, BASE I 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, BASE I checks the transaction amount against the Total Cash activity limits. If the transaction passes the Total Cash check, BASE I increments the Total Cash count and amount accumulators and approves the transaction.

If the ATM sublimits are greater than the Total Cash limit, STIP uses the sublimits instead of the Total Cash limit.

Quasi-Cash and Other Cash—BASE I uses the Total Cash activity limits. BASE I checks Quasi-Cash and Other Cash transactions against the activity limits the issuer establishes for

Total Cash and updates activity accumulators for Quasi-Cash and Other Cash 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.

5.7.3 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.

5.8 HIGH-PRIORITY RESPONSE CODE SELECTION

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.
- Expiration date edit response code.
- CVV or iCVV response code.
- CAVV response code.
- dCVV response code.
- Exception file response code.

5.9 FORWARD-REFERRAL DECISION

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.

5.9.1 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 PCR level to accept forward referrals.
  - The response code must indicate that the transaction is eligible for forward-referral.
- For Card Verification Value (CVV) Service processing, if the issuer chooses the “All Respond” option, V.I.P. validates the CVV or iCVV; if the validation fails, V.I.P. responds to the acquirer with the issuer's invalid CVV/iCVV response code.
- For Card Verification Value 2 (CVV2) Service processing, if the issuer chooses the “CVV2 All” option, V.I.P. validates the CVV2; if the validation fails, V.I.P. forwards the request to the issuer with the CVV2 in Field 126.10—CVV2 Authorization Request Data. If the issuer is unavailable, V.I.P. responds to the acquirer with the issuer's CVV2 response code.
- The transaction is an address verification transaction, for which VisaNet performs address verification and forwards the result to the issuer. The issuer option at the PCR level to accept forward referrals does not apply.
- The transaction is an ATM cancellation (or reversal) transaction.
- The transaction is a MOTO/EC transaction in which the expiration date is not present and the issuer chooses not to process MOTO/EC transactions in STIP without an expiration date.
- The account number length is invalid (not one of the card lengths specified for the issuer BIN).

5.9.2 “No Forward-Refer” Processing

If a transaction does not qualify for forward-referral, V.I.P. 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:
  - If the transaction is not made with a Visa card, STIP changes the exceeds limits response code to **01** (referral).
  - If the transaction is made with a Visa card, STIP checks the merchant category code (MCC) table. If the table indicates to change referral responses to denial, STIP sets the response code to **05**. Otherwise, STIP sets the response code to **01** (referral).
- If the transaction exceeds the activity amount or count, and the account is a Visa Electron account, STIP forces the response code to **05**.

5.10 ACTIVITY UPDATE

STIP updates the count and amount activity information in the activity file under the following conditions:

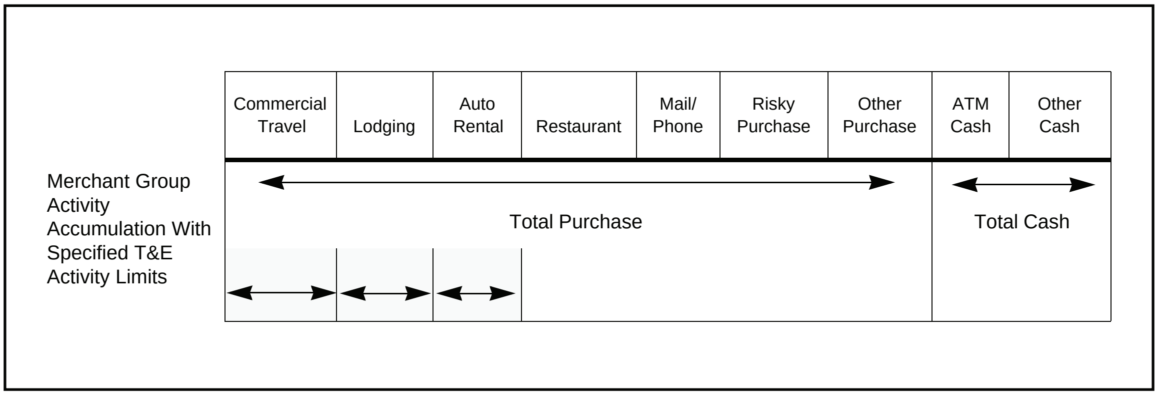
- The transaction is approved in STIP.
- The transaction is an authorization and not a repeat (message type 0101).
- The transaction is not a verification transaction.
- The transaction is not below the advice limit.
- The transaction is between advice and issuer limits and the issuer chose to have STIP check activity.

See “Reversal Processing” in this chapter for information about processing reversals.

V.I.P. 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, V.I.P. accumulates activity once for the MCG only.

For example, Figure 5-3 illustrates how V.I.P. accumulates activity for an issuer that has selected separate activity limits for Commercial Travel, Lodging, and Auto Rental MCG transactions. V.I.P. accumulates activity in any of these groups for that group and for Total Purchase.

Figure 5-3 Example of Activity Accumulation



5.11 ADVICE CREATION

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 check acceptance transactions.
  - For transactions receiving any of the response codes listed in Table 5-6.

Table 5-6 No-Advice STIP Decline Response Codes

Response Code	Explanation
06	Error
12	Invalid transaction
13	Invalid amount
14	Invalid account
15	No such issuer
28	File temporarily unavailable
57	Transaction not permitted to cardholder
62	Restricted card; restricted between certain countries
63	Security violation

Table 5-6 No-Advice STIP Decline Response Codes (continued)

Response Code	Explanation
78	No account
81	PIN cryptographic error found
96	System malfunction
N3	Cash 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.
  - If the issuer participates in the Positive Authorization Capacity Management (PACM) Service.
  - For Discover, Diners Club, and JCB transactions.

  NOTE

  STIP creates advices for all non-approved PCAS transactions.

Table 5-7 shows how STIP determines whether to create advices for non-approved PCAS and PACM between-limit transactions.

Table 5-7 Advice Creation for Non-Approved PCAS and PACM 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 transactiona and all PACM transactions.

5.12 RESPONSE CODE CONVERSION

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, V.I.P. converts it to **05** but sends code **75** to the issuer in the 0120 advice. If the issuer returns code **75** in the 0110 response, V.I.P. forwards it unchanged to the acquirer; otherwise, V.I.P. inserts 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

For the Visa Europe (VE) region, STIP converts all referral response codes to declines regardless of the dollar amount.

- When STIP creates an advice for the issuer, STIP inserts the original, unconverted response code in field 39 of the advice.

5.12.1 Converting Over-Limit and Referral Codes in Acquirer Responses

STIP converts over-limit response codes **61** and **65** to approval or decline response codes as the issuer processing center specifies. Table 5-8 contains conversion details.

Table 5-8 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-U.S. issuers may specify referral code **01** except for Visa Electron transactions, which cannot be referred per Visa International Operating Regulations.
	ATM transaction referrals	Decline code **05**.

Stand-In Processing (STIP)

Table 5-8 Converting Over-Limit and Referral Codes (continued)

Response Code	Condition	Converted to...
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. See "Field 39—Response Code" in *V.I.P. System BASE I Technical Specifications, Volume 1*, for more information.
75	Exceeds PIN-entry retry limit (any transaction)	Decline code **05**.[1]

[1] Although V.I.P. converts code **75** to code **05**, V.I.P. forwards code **75** to issuers in 0120 advices. If an issuer returns the 0110 response with code **75** in field 39, VisaNet forwards it unchanged to the acquirer. Otherwise, V.I.P. inserts 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 5-9 contains these conversion details.

Table 5-9 Converting Approval, Forward-or-Approve/Decline, or Incorrect CVV or iCVV Response Codes

Response Code	Condition	Converted to...
11	**VIP** (Very Important Person) approval (authorization request)	Approval code **00**.
A–A9	**VIP** approval (account number verification—Visa U.S.A. only)	Not declined, code **85**.
XA	Forward or approve (authorization request)	Approval code **00**.
	Forward or approve (account number verification—Visa U.S.A. 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: • Approval code **00** • Referral code **01** • Pick Up code **04** • Decline code **05**

Acquirers receive declines (code **05**, do not honor) 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 5-10 defines the processing rules for referral response codes.

NOTE

In the Visa Europe (VE) region, these referral-to-decline conversion rules apply to domestic transactions as well as to regional and interregional transactions.

Table 5-10 Referral Response Code Processing Rules

Condition	Rule
STIP processes the transaction and all of the following is true: • The STIP-generated referral response code is **01** or **02**.[1] • The issuer is available and the STIP parameter indicates that the issuer accepts forward referrals. • 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.	VisaNet forwards the transaction to the issuer for authorization.
STIP processes the transaction and all of the following is true: • The STIP-generated referral response code is **01** or **02**. • The issuer is available and the STIP parameter indicates that the issuer does not want forward referrals. *or* • The issuer is unavailable. • 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.	V.I.P. 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: • The POS condition code is **08**. • The POS condition code is **02** (unattended terminal). • The MCC in Field 18—Merchant Type indicates a MOTO, AFD, computer network services, or door-to-door sales transaction. • The MCC in field 18 indicates a transaction from an impractical merchant environment as defined in the *Visa International Operating Regulations*, and the transaction amount is equal to or less than USD$100.00.	V.I.P. 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 code **01** to the acquirer in the response. Only the issuer can send code **02** to the acquirer in the response.

5.13 REVERSAL PROCESSING

BASE I does not match a reversal to the original. BASE I also does not know how the original was processed—whether it was processed by the issuer or by STIP. BASE I 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.

5.13.1 Activity Testing on Reversals

V.I.P. performs Positive Cardholder Authorization Service (PCAS) activity testing in stand-in processing (STIP) for reversals as follows. Unlike processing for originals, V.I.P. does not test reversal activity against preset issuer activity limits. For a reversal, V.I.P. 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). V.I.P. checks the CDB for originals containing amounts greater than or equal to the reversal's cardholder billing amount.

During STIP reversal processing, V.I.P. 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 V.I.P. can determine that the reversal's corresponding original activity is present in the CDB, V.I.P. prepares to respond with response code **00** (reversal approved—original located in CDB). For ATM reversals, V.I.P. also subtracts the cardholder billing amount, in U.S. dollars, from the CDB.

NOTE

Partial reversals do not apply to ATM transactions.

When V.I.P. cannot determine that the reversal's corresponding original activity is present in the CDB, V.I.P. prepares to respond with response code **21** (reversal approved—original not located in CDB), indicating that V.I.P. 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 V.I.P. processing or transaction settlement. V.I.P. 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.

Chapter 6

The Cardholder Database, Merchant Central File, and Advice File

The Cardholder Database (CDB), the Merchant Central File (MCF), and the Advice File reside at each VisaNet Interchange Center (VIC). V.I.P. is responsible for ensuring the integrity of all system files. To manage information in the files, V.I.P. accepts a file update only from the issuer responsible for the set of card numbers in the message.

V.I.P. 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.

VisaNet 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 and in the Merchant Central File.

The Cardholder Database and the Merchant Central File contain the following files:

- Exception File
- PIN Verification File
- Address Verification File
- Merchant Central File
- Portfolio File
- Risk-Level File
- Card-Level Product ID

6.1 CARDHOLDER DATABASE FILES

The *BASE I Cardholder Database (CDB)* contains cardholder information that stand-in processing (STIP) uses to authorize transactions and to verify accounts, addresses, and personal identification numbers (PINs). The CDB also contains Positive Cardholder Authorization Service (PCAS) limits and Positive Authorization Capacity Management (PACM) Service limits for individual cardholders.

The Cardholder Database contains the following files:

- Activity File
- Address Verification File
- Exception File
- PIN Verification File
- Portfolio File
- Risk-Level File
- Account-Level Processing (ALP) ID File

Visa is responsible for maintaining the activity (and advice) files; issuers are responsible for establishing and for maintaining the rest.

6.1.1 Database Content

The following figure shows the layout for each file in the Cardholder Database.

Cardholder Database Files

Activity File (Visa-Maintained)

Account Number Length	Cardholder Account Number	Purge Date	Country Code	Issuer ID Length	Issuer ID	Purchase Activity	Cash Activity	Daily Spending	Monthly Spending	Invalid PINs

Address Verification File (Issuer-Maintained)

Account Number Length	Cardholder Account Number	Purge Date	Country Code	Issuer ID Length	Issuer ID	Postal Code	Address Verification Value	Update Time	Effective Time

Exception File (Issuer-Maintained)

Account Number Length	Cardholder Account Number	Purge Date	Country Code	Issuer ID Length	Issuer ID	Action Code	Region Coding	Update Time	Effective Time

PIN Verification File (Issuer-Maintained)

Account Number Length	Cardholder Account Number	Purge Date	Country Code	Issuer ID Length	Issuer ID	PIN Verification Data	Update Time	Effective Time

Portfolio File (Issuer-Maintained)

Account Number Length	Cardholder Account Number	Amount	Acquiring Institution Country Code	Card Acceptor ID	Card Acceptor Name	Trans ID	Merchant Verification Value	Purge Date	Type of Stop Order	Cardholder Name
Merchant Account Number										

Risk-Level File (Issuer-Maintained)

Account Number Length	Cardholder Account Number	Purge Date	Country Code	Issuer ID Length	Issuer ID	Risk Level	Daily Spending Limit	MCG Activity Limits	Update Time	Effective Time

Account-Level Processing (ALP) ID File (Issuer-Maintained)

Account Number Length	Cardholder Account Number	Purge Date	Country Code	Issuer ID Length	Issuer ID	Activation Date	Account Product ID	Rewards Program ID

6.1.2 File Record Formats and Update Methods

Table 6-1 lists the file types for the Cardholder Database files.

Table 6-1 File Record Formats and Update Methods

File	Format	Name/Type
Address Verification File	Format 2	A2
BASE I 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 (issuer institution ID *or* country code fields are applicable)	Format 2	E2
Merchant Central File	Format 2	M9
PIN Verification File	Format 2	P2
Portfolio File	Format 2	PF
Risk-Level File	Format 2	R2
Card-Level Product ID	Format 2	n/a

See the end of this chapter for additional information about online file updating.

6.1.3 Fields Common to All Issuer-Maintained CDB Files

Table 6-2 lists the fields common to all of the issuer-maintained CDB files. The individual file sections do not repeat their descriptions.

Table 6-2 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: • 13- or 16-digit numeric bankcard numbers • 5–28-digit numeric bank card numbers and proprietary card numbers • 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*). V.I.P. determines purge date centuries as follows: • If *YY* = **00–49**, then the century is the 21st (years 2000 through 2999) • If *YY* = **50–99**, then the century is the 20th (years 1900 through 1999) **NOTE:** *V.I.P. rejects exception file records submitted with purge date years 2042 through 2098.* See the individual Cardholder Database file descriptions in this chapter 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. V.I.P. uses this field, along with the issuer institution ID field, to identify the issuer.

Table 6-2 Fields Common to All Issuer-Maintained CDB Files (continued)

Field	Purpose
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 V.I.P. cannot determine it from the cardholder account number. V.I.P. requires this field for proprietary card and private-label card numbers if the account range duplicates that of another issuer's accounts. V.I.P. uses the field with the country code field to identify the issuer processor. Issuers must prearrange with Visa 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.
Update Time	Update time is a system-generated “time stamp” indicating the date and time that VisaNet establishes a record. Update time is not visible to users but is available to Visa staff for research and for settling chargeback disputes. V.I.P. 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. For the Exception File, update time refers to the first date and time V.I.P. updates the file with a pick-up code, that is, non-approval codes **01**, **04**, , **07**, **41**, or **43**. V.I.P. 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.

6.2 ACTIVITY FILE

6.2.1 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)

Issuers can optionally choose to not have the cardholder’s four-day activity count tested, but BASE I always tests the four-day activity amount.

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.

6.2.2 File Content

The Activity File organizes records by cardholder account number. Each cardholder record contains accumulators for:

- Merchant group activity.
- Invalid PIN-entry activity.

The following figure illustrates the basic structure of an Activity File record.

Activity File Record Layout

Activity Record				
Purchase Activity	Cash Activity	Daily Spending	Monthly Spending	Invalid PINs

6.2.3 Unique Fields

The following subsections describe the fields unique to the Activity File and their uses.

6.2.3.1 Purchase and Cash Merchant Group Activity

Activity File records contain accumulated merchant category group (MCG) activity counts and dollar 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 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. VisaNet does not maintain separate issuer-available counts and issuer-unavailable counts.

The following figure illustrates the relationship between activity records and MCGs.

Activity Record Layout—Purchase Activity MCG Breakdown

Purchase Activity by MCGs							
	Commercial Travel	Lodging	Auto Rental	Restaurant	MOTO/EC	Risky Purchase	Total Purchase
1-Day Amount Totals							
1-Day Count Totals							
4-Day Amount Totals							
4-Day Count Totals							

As shown in the following figure, the cash activity portion of the activity record is divided into two cash MCGs.

Activity Record Layout—Cash Activity MCG Breakdown

Cash Activity by MCGs		
	Total Cash	ATM Cash
1-Day Amount Totals		
1-Day Count Totals		
4-Day Amount Totals		
4-Day Count Totals		

6.2.3.2 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 the following figure. When the number of attempts equals the issuer-specified PIN-entry retry limit, STIP declines the transactions (but does not request pick-ups). V.I.P. resets the invalid PIN accumulator to zero at 00:00 hours.

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.

6.2.3.3 Velocity Limits

Recipient issuers that support enhanced OCTs can opt to participate in velocity limit checking. There are three count and three amount limits for domestic transactions and for cross-border transactions. VisaNet can use these limits on behalf of the recipient issuer during an OCT transaction and, if the limit is exceeded, VisaNet can either decline the OCT on the recipient issuer’s behalf or forward the OCT to the recipient issuer with information about the exceeded limit.

Visa increments the counts and amounts only for approved enhanced format OCTs sent to recipient issuers that support enhanced format.

The table below provides the following information on domestic limits:

- **Limit Category** — Count limit or amount limit
- **Limit Timeframe** — 1–day, 7–day, or 30–day

- **Issuer Limit Rule** — The rules that issuers need to follow when defining their limits.
- **Maximum/Default Value** — The maximum value for the limit, which is also the Visa-defined default. Participating issuers can modify the limits.

Table 6-3 Domestic Limits

Limit Category	Limit Timeframe	Issuer Limit Rule	Maximum/Default Value
Count Limit	1–day	Must be equal to or less than 150 transactions	150 transactions
	7–day	Must be equal to or greater than the 1–day count limit Must be equal to or less than 250 transactions	250 transactions
	30–day	Must be equal to or greater than the 7–day count limit Must be equal to or less than 750 transactions	750 transactions
Amount Limit	1–day	Must be equal to or less than USD$100,000	USD$100,000
	7–day	Must be equal to or greater than the 1–day amount limit Must be equal to or less than USD$250,000	USD$250,000
	30–day	Must be equal to or greater than the 7–day amount limit Must be equal to or less than USD$500,000	USD$500,000

The table below provides the following information on cross-border limits:

- **Limit Category** — Count limit or amount limit
- **Limit Timeframe** — 1–day, 7–day, or 30–day
- **Issuer Limit Rule** — The rules that issuers need to follow when defining their limits.
- **Maximum/Default Value** — The maximum value for the limit, which is also the Visa-defined default. Participating issuers can modify the limits.

Table 6-4 Cross Border Limits

Limit Category	Limit Timeframe	Issuer Limit Rule	Maximum/Default Value
Count Limit	1–day	Must be between 1 and 30 transactions	30 transactions
	7–day	Must be equal to or greater than the 1–day count limit Must be between 5 and 50 transactions	50 transactions

Table 6-4 Cross Border Limits (continued)

Limit Category	Limit Timeframe	Issuer Limit Rule	Maximum/Default Value
	30–day	Must be equal to or greater than the 7–day count limit Must be between 10 and 150 transactions	150 transactions
Amount Limit	1–day	Must be between USD$2,500 and USD$20,000	USD$20,000
	7–day	Must be equal to or greater than the 7–day amount limit Must be between USD$5,000 and USD$50,000	USD$50,000
	30–day	Must be equal to or greater than the 30–day amount limit Must be between USD$10,000 and USD$100,000	USD$100,000

Recipient issuers can either define a value for the limit following the rules outlined in the above table or use the default value defined by Visa.

NOTE

Recipient issuers do not need to participate in these velocity limits. If a recipient issuer does not choose to participate in these velocity limits, the limits will not be used on their transactions.

The recipient issuer's velocity limits will be set for individual accounts at the BIN level. For example, if the domestic 1-day count limit for a BIN is set to a maximum of five transactions, every card account for the BIN is allowed to have up to five enhanced money transfer OCTs per day.

When the limit is exceeded and the issuer is unavailable, Visa will decline the OCT.

When the limit is exceeded and the issuer is available, the issuer has two options:

- The issuer can have VisaNet forward the OCT to them with information in it related to the exceeded velocity limit.
- The issuer can have VisaNet decline the OCT on their behalf.

When the issuer has opted for VisaNet to forward them the OCT when the velocity limit is exceeded, the issuer must be prepared to receive Field 48: Usage 37, position 11. This field will contain the following velocity limit related information that the issuer can use in making their authorization decision:

- 1 = 1-day count or amount exceeded
- 2 = 7-day count or amount exceeded
- 3 = 30-day count or amount exceeded

NOTE

V.I.P. will populate this field with the priority order of 1, 2, and then 3.

When VisaNet declines a transaction based on velocity limits, it creates a STIP advice if the issuer is set up to receive STIP advices.

Recipient issuers communicate their velocity limit options via the Customer Information Questionnaire (CIQ). Contact your Visa representative for details.

6.2.4 Maintenance and Update

Once a day, at 00:00 hours, VisaNet updates the Activity File by “rolling over” transaction accumulators so that the file always reflects four days of current activity.

VisaNet clears invalid PIN counts daily. Also, as long as invalid PIN-entry activity is under the limits, VisaNet 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. Refer to the PIN Verification Service (PVS) chapter in *V.I.P. System Services, Volume 2*, for further information about excessive PIN-entry attempt processing.

6.2.5 Purging Records

Members do not purge records from the Activity File. VisaNet performs this task.

6.3 ADDRESS VERIFICATION FILE

6.3.1 File Description

V.I.P. uses the *Address Verification File (AVF)* to verify a cardholder address in card-present and card-not-present authorization requests. V.I.P. compares the cardholder address to the address information in the AVF for the account.

6.3.2 File Content

The AVF contains records organized by account number. The following figure illustrates the AVF record layout.

Address Verification File Record Layout

Account Number Length	Cardholder Account Number	Purge Date	Country Code	Issuer ID Length	Issuer ID	Postal Code	Address Verification Value	Update Time	Effective Time

6.3.2.1 Postal Code

This field contains either the cardholder's 5- or 9-digit postal or ZIP code. If the issuer uses five digits of the ZIP code, they must left-justify the five digits and zero-fill the remainder of the field.

6.3.2.2 Address Verification Value

This field contains up to five digits of the cardholder's street address. Issuers must left-justify the contents of this field space-fill the remainder. Issuers express numeric street names in numeric form, for instance, issuers express “Third Street” as “3 Street”.

The issuer provides the address data using one of the two Visa compression algorithms, *leading numerics* or *first five numerics*, that is, the same compression method the issuer wants VisaNet to use when sending address data to the issuer for verification. If, for instance, the issuer is using leading numerics, VisaNet sends and stores in the cardholder's AVF record the address “123 4th Street” as “123”. If the issuer uses the first five numerics algorithm, VisaNet sends and stores the address “123 4th Street” as “1234.”

The algorithms ignore the following characters if they are within the first five numerics:

/ (forward slash)

**** (back slash)

(pound or number sign)

- (hyphen)

The Field 123, Address Data, section of *V.I.P. System BASE I Technical Specifications, Volume 1*, summarizes the compression methods and the address-matching algorithms. Also refer to *V.I.P. System Services, Volume 2*, for more information about the Address Verification Service (AVS).

6.3.3 Maintenance and Update

Issuers maintain and update address information in this file. See “File Maintenance Methods” in this chapter for information about update methods.

6.3.4 Purging Records

Issuers maintain and update address information in this file.

6.4 EXCEPTION FILE

6.4.1 File Description

The *Exception File* is a VIC-resident, online file containing cardholder account records. V.I.P. accesses the file during STIP processing. Reasons for Exception File-based responses include:

- V.I.P. 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 U.S. region, acquirer processors should call the International Automated Referral Service (IARS).
- The issuer processor should process the request when possible.
- V.I.P. should approve transactions on this account regardless of cardholder activity.
- To prevent cards from being used in certain countries.

Exception File—V.I.P. uses this 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. 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, V.I.P. 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. Refer to "Region Coding" in this chapter 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]). U.S.-region CRBs also contain accounts with negative action code **05** (do not honor),*

6.4.1.1 Generating Visa Card Recovery Bulletins (CRBs)

BASE I extracts data from the Exception File for the Card Recovery Bulletin (CRB) Service to use 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, or either decline them in the U.S. region only.

Issuers submit updates to the Exception File through their VisaNet connection by using an update tape, by using Visa Resolve Online (VROL), or by using the Automated Cardholder Database Update (Auto-CDB) Service. 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 Center Records (PCRs).

Refer to *V.I.P. System Services, Volume 2*, for information about the CRB Service and about the Auto-CDB Service.

6.4.2 File Content

The Exception File contains records organized by account number, as illustrated in the following three figures. V.I.P. generates the update time, the effective time, the service indicators, and the history indicators.

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

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

6.4.3 Unique Fields

The following subsections describe the unique Exception File fields.

6.4.3.1 Action Codes

Each Exception File record must contain one of the action codes for Field 127—File Maintenance listed in Table 6-5. See *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for more information about this field and about valid action codes.

Table 6-5 Exception File Action Codes

<table>
<tr><th>Code</th><th colspan="4">Definition</th></tr>
<tr><td>01</td><td colspan="4">Refer to card issuer</td></tr>
<tr><td>04</td><td colspan="4">Pick up card</td></tr>
<tr><td>05</td><td colspan="4">Do not honor
NOTE:
<i>This negative response code only causes U.S.-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.</i></td></tr>
<tr><td>07</td><td colspan="4">Pick up card, special condition</td></tr>
<tr><td>11</td><td colspan="4">Approval for <b>VIP</b> (Very Important Person)</td></tr>
<tr><td>41</td><td colspan="4">Lost card, pick up</td></tr>
<tr><td>43</td><td colspan="4">Stolen card, pick up</td></tr>
<tr><td colspan="5">Codes <b>A1</b> through <b>A9</b> are <b>VIP</b> codes associated with special high-value activity limits. Amount limits are in United States (U.S.) dollars.</td></tr>
<tr><td rowspan="2"></td><th colspan="2">One-Day Limits</th><th colspan="2">Four-Day Limits</th></tr>
<tr><th>Amount</th><th>Count</th><th>Amount</th><th>Count</th></tr>
<tr><td>A1</td><td>USD$1,500</td><td>3</td><td>USD$1,500</td><td>9</td></tr>
<tr><td>A2</td><td>USD$2,000</td><td>5</td><td>USD$3,500</td><td>12</td></tr>
<tr><td>A3</td><td>USD$3,000</td><td>8</td><td>USD$6,000</td><td>14</td></tr>
<tr><td>A4</td><td>USD$4,500</td><td>12</td><td>USD$8,000</td><td>25</td></tr>
<tr><td>A5</td><td>USD$6,000</td><td>15</td><td>USD$10,000</td><td>40</td></tr>
<tr><td>A6</td><td>USD$8,000</td><td>20</td><td>USD$14,000</td><td>50</td></tr>
<tr><td>A7</td><td>USD$10,000</td><td>25</td><td>USD$20,000</td><td>100</td></tr>
<tr><td>A8</td><td>USD$1,500</td><td>4</td><td>USD$2,000</td><td>10</td></tr>
<tr><td>A9</td><td>USD$2,225</td><td>6</td><td>USD$3,500</td><td>13</td></tr>
<tr><td>XA</td><td colspan="4">Forward to issuer; default to <b>00</b></td></tr>
<tr><td>XD</td><td colspan="4">Forward to issuer; default to <b>05</b></td></tr>
</table>

The field 127 codes are valid for file updates. The 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. VisaNet allows only one action code per record.

V.I.P. 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 V.I.P. routes the transaction to STIP.

6.4.3.2 Region Coding

Each Exception File record must contain one of the region codes for field 127 listed in Table 6-6. See *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for information about this field and valid action codes.

Table 6-6 BASE I CRB Region Codes

Region Code	Geographic Area
0	No Bulletin/V.I.P. Only (cannot be combined with any other region code)
A	All countries in the Asia-Pacific region
B	All countries in the Central Europe, Middle East, and Africa (CEMEA) region
C	All Visa Canada
D	National Card Recovery Bulletin
E	All countries in Visa Europe
F	All countries in the Latin America and Caribbean (LAC) region

Issuers use region codes to specify the geographical areas in which they want the cardholder's account number 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-U.S. users). However, the CRB Service includes region **0** accounts in the *NCRF* (the electronic version of pick-up listings available to U.S. member processors).

Issuers use region code **E** to include the account in the Visa Europe CRB. Issuers use code **E** for all electronic STIP authorizations regardless of the region in which the acquirer processor or the issuer processor is located.

IMPORTANT

*Visa eliminated the U.S. region CRB; issuers and VisaNet do not use the codes **X1** (region **1**) through **X9** (region **9**).*

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**. VisaNet 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, see the Card Recovery Bulletin (CRB) Service chapter in *V.I.P. System Services, Volume 1*, and the *Card Recovery Bulletin Service User's Guide*.

Canada Region Codes C1–C3

VisaNet no longer supports Canada subregion codes **C1**–**C3**.

6.4.4 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.

6.4.4.1 VisaNet Connection

Issuers equipped with a VisaNet 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 VisaNet, such as the effective time field.

Issuer processors can request a record at any time while signed on to the network, although VisaNet may restrict file access to low-volume hours. Issuer processors must be authorized to access the file. For programming details, see the description of file inquiry message type 0302 in *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

Online Exception File Editing Summary (0302 Messages)—Members can maintain their exception records without knowing the current status of the record on the V.I.P. files.

- V.I.P. accepts attempts to add a record for a cardholder that is already on the file as changes.
- V.I.P. accepts attempts to change a record for a cardholder that is not already on the file as additions.
- V.I.P. rejects attempts to delete a record that is not on the file with error code **565** (no record on file).
- V.I.P. 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). An out-of-synchronization condition does not affect the update task.

Which file types issuers can use depends on the sending station.

BASE I 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 6-7 summarizes the Exception File update processing actions.

Table 6-7 Exception File Update Processing Actions

Action/File Type	Card Number Valid—Not Present on File Result	Card Number Valid—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

Table 6-7 Exception File Update Processing Actions (continued)

Action/File Type	Card Number Valid—Not Present on File Result	Card Number Valid—Present on File Result
Change E4	Add to File	

Table 6-8 summarizes the Exception File update processing actions.

Table 6-8 V.I.P.-Format Exception File Update Processing Actions

	BASE I Invalid/SMS Invalid	BASE I Invalid/SMS Valid	BASE I Invalid/SMS Present	BASE I Valid/SMS Valid	BASE I Valid/SMS Present	BASE I Present/SMS Valid	BASE I Present/SMS Present
Action/File Type	**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** **0572**						
Delete E4	**0571** **0572**						

For further information, refer to the Cardholder Database chapter in *V.I.P. System Services, Volume 2*.

6.4.4.2 Using Telephone, Telex, or Fax Machines for Updates

Issuer processing centers without direct network links can update the Exception File through V-SAFE, which has an online link to BASE I. Linked issuer processors can contact Global Customer Assistance Services (GCAS) for emergency updates during an issuer processor system failure.

The following limitations apply to telephone, telex, and fax requests:

U.S. Issuer Processors—Issuers can request manual updates for emergency purposes or for **VIP** accounts only. Issuers can request up to 100 updates by telex or by fax machine.

Non-U.S. 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 telex or 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: CENTER 4 EXCEPTION FILE.
2. The country in which the issuer processor is located.
3. The update information, grouped according to update transaction code:

   EA = Add

   EC = Change

   ED = Delete

   The cardholder account number

   The response code or forwarding code, if the request is for an addition or for a change:

   01 = Refer to card issuer

   04 = Pick up card

   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 center ***or*** approve transaction

   XD = Forward request to center ***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 member processing center's telex, fax, or telephone number.

6.4.4.3 Automatic Cardholder Database Update (Auto-CDB) Service

In addition to using 03*xx* 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 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.

V.I.P. replaces the old Exception File information with the new information before it sends the 0110 response to the acquirer. V.I.P. also creates an issuer advice. When V.I.P. 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**), VisaNet checks the Exception File to determine if it lists the cardholder account. If the file does not list the account, VisaNet automatically adds the account to the file with the applicable pick-up code and with region code **0**. If the file lists the account with a code other than a pick-up code, V.I.P. changes the listing to pick-up status.

V.I.P. only processes an update when the authorization response includes a valid field 39 response code and a valid field 127 file action code. Table 6-9 lists valid response code and file action code combinations.

Key to Table

X indicates a valid combination, and VisaNet 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 VisaNet 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 6-9 Valid Response Message Field Combinations for Exception File Updates

	File Action Code (ISO 127.E)								**Update Code (ISO 91)**	
Authorization Response (ISO 39)	**Refer**	**Pick Up**	**Decline**	**Pick Up Special**	**Pickup Lost Card**	**Pick Up Stolen**	**Switch to Issuer; Approve if Unavail.**	**Switch to Issuer; Deny if Unavail.**	**Replace**	**Delete**
	01	**04**	**05**	**07**	**41**	**43**	**XA**	**XD**	**4**	**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 (U.S.-donestic 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	

6.4.4.4 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 V-SAFE forwards an advice of the Exception File update to the issuer processor so the issuer can delete or change the exception record as needed.

6.4.4.5 Reports

V.I.P. 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)
- Report BIOPPCSD—Preauthorized Payment Cancellation Service Daily Activity Detail Report

For information about these reports, refer to *V.I.P. System Reports*.

6.4.4.6 Raw Data Files

V.I.P. also produces two member-subscription Exception File raw data files:

- BIOSRUP—Exception File Update File
- BIOSRLP—Exception File Listing File

Using transaction code **33**, the V.I.P. System transmits these files to the member processors through the BASE II System. Refer to *V.I.P. System Reports* for report descriptions and samples. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for information about raw data files.

6.4.5 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.

6.4.5.1 Purge Date Formats

The Exception File stores only one purge date at a time for an account. This date corresponds to the expiration date of the applicable bulletin for the country in which the account is listed.

Purge Date

For additions and changes to Exception File records, V.I.P. converts the purge date to coincide with the expiration 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 nonexpiring purge date of **999900**, V.I.P. converts the date to the date of the update request plus 20 years.

6.4.5.2 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.
- If the issuer does not supply a purge date for an Enhanced Auto-CDB update (available only for the Exception File), the default is the transaction date plus 60 days.

See the *Card Recovery Bulletin Service User's Guide* for more purge date considerations.

Refer to “File Maintenance Methods” in this chapter for file update information.

6.5 PIN VERIFICATION FILE

6.5.1 File Description

Authorization requests include personal identification numbers (PINs) when cardholders use them at the point of service or point of sale (POS) 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.

6.5.2 File Content

The *PIN Verification File* contains records organized by account number. The following figures illustrate a format 1 file record and a format 2 file record.

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		

6.5.3 Unique Fields

This subsection describes the unique PIN Verification File data fields.

6.5.3.1 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 Visa PIN Verification Service (PVS) cannot verify the PIN. If the issuer specifies that V.I.P. is to perform PIN verification for a specific account range, and an individual card has a PVKI of **0**, V.I.P. 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.

6.5.3.2 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

Data Encryption Standard (DES) 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 DES and an IBM PIN offset algorithm. For additional details, refer to the *Payment Technology Standards Manual*.

6.5.4 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.

6.5.5 Purging Records

Issuers control record purging by specifying purge dates. The format for purge dates in this file is *YYMMDD*. V.I.P. 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.

Refer to *V.I.P. System Services, Volume 2*, for information about the PIN Verification Service.

6.6 PORTFOLIO FILE

6.6.1 File Description

The *Portfolio File* contains issuer-supplied stop payment orders for preauthorized payment transactions. The U.S. region-only Preauthorized Payment Cancellation Service (PPCS) uses this file.

- Cardholders initiate *stop payment orders*, and PPCS enables issuers to stop electronic funds transfers for a specific recurring payment or for an installment payment transaction for a specific account from a particular merchant when requested by the cardholder.
- For *revocation of authorization orders*, PPCS enables issuers to stop all future electronic funds transfers for recurring or installment payment transactions for a specific account from a particular merchant when requested by the cardholder.

When VisaNet receives a preauthorized payment authorization request, V.I.P. checks the Portfolio File to see if there is a stop payment order on file. If it does not find a match, V.I.P. continues processing the request. If V.I.P. does find a match, it declines the transaction on behalf of the issuer with stop order code **R0** (stop payment order), stop order code **R1** (revocation of authorization order), stop order code **R3** (revocation of all authorizations order), or stop order code **C2** (revocation of all authorizations order) in Field 39—Response Code.

NOTE

*Only BASE II users use the **C2** stop-order code.*

6.6.2 File Content

Issuers update the records by 0302 messages using a tag-length-value (TLV) field format for the type of stop order, the cardholder name, and the merchant account number. V.I.P. obtains other record information, such as the transaction identifier (TID), from other fields in the 0302 message. Refer to the field 127 description in *V.I.P. System BASE I Technical Specifications, Volume 1*, for details about submitting Portfolio File data.

The following figure illustrates a Portfolio File record layout.

Portfolio File Record Layout

Account Number Length	Cardholder Account Number	Amount	Acquiring Institution Country Code	Card Acceptor ID	Card Acceptor Name/Location	Trans ID	Merchant Verification Value

Purge Date	Type of Stop Order	Cardholder Name	Merchant Account Number

6.6.3 Unique Fields

The following fields are unique to the Portfolio File.

NOTE

VisaNet requires the record purge date in 0302 addition requests.

6.6.3.1 Amount

This field contains the specific stop payment amount. VisaNet requires the amount for stop payment orders, but it is optional for revocations. If the issuer does not supply the amount in the 0302 request, V.I.P. does not use the amount in transaction matching.

6.6.3.2 Acquiring Institution Country Code

This code identifies the country of the acquirer. VisaNet requires this code in 0302 addition requests.

6.6.3.3 Card Acceptor ID

The card acceptor ID identifies the merchant initiating the recurring or installment payment transaction. This 15-byte-maximum EBCDIC value comes from Field 42—Card Acceptor Identification Code in the original request. VisaNet requires this field, or the merchant verification value (MVV), in 0302 add or replace requests (Field 91—File Update Code contains **1** or **4**); otherwise, it is optional.

6.6.3.4 Card Acceptor Name/Location

The card acceptor name/location identifies the merchant initiating the preauthorized payment transaction. This field is optional in 0302 add or replace requests (field 91 contains **1** or **4**). It should not appear in 0302 delete or inquiry requests (field 91 contains **3** or **5**).

6.6.3.5 Transaction Identifier

The *transaction identifier (TID)* is a right-justified, VisaNet-generated identifier in field 62.2 that is unique for each original transaction. V.I.P. assigns a TID to all transactions. PPCS issuers may provide a TID for addition requests; if the issuer does not provide a TID in an addition request, V.I.P. assigns one and returns it in the request. VisaNet requires the TID in 0302 delete, replace, or inquire requests. This field must be copied in 0400 reversal requests from the original 0110 response, if it was present in the original response.

6.6.3.6 Merchant Verification Value (MVV)

The MVV uniquely identifies the merchant. This 5-byte value comes from field 62.20 in the original request. VisaNet requires this field, or the card acceptor ID, in 0302 add or replace requests (field 91 contains **1** or **4**); otherwise, it is optional.

6.6.3.7 Type of Stop Order

This field contains the stop-order code. VisaNet requires a stop-order code in 0302 add requests; it is optional for delete requests. Valid values are:

- **R0** = Stop-payment order
- **R1** = Revocation of authorization order
- **R3** = Revocation of all authorizations order
- **C2** = Revocation of all authorizations order

NOTE

*Only BASE II users use the **C2** stop-order code.*

6.6.3.8 Cardholder Name

This field is a 23-byte-maximum, EBCDIC field that contains the cardholder's name. This field is optional.

6.6.3.9 Merchant Account Number

This field is a 27-byte-maximum, EBCDIC field that contains the merchant's account number. This field is optional.

6.6.4 Maintenance and Update

Issuers are responsible for maintaining and for updating Portfolio File records.

6.6.5 Purging Records

Issuers provide a purge date for all Portfolio File records.

6.7 RISK-LEVEL FILE

6.7.1 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.

6.7.2 File Content

The following figures illustrate a risk-level file record. The data 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.

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

Risk-Level Record Layout—Daily Spending Limits Breakdown

Daily Spending Limits			
Non-Cash Limit		Cash Limit	
Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable

Risk-Level Record Layout—MCG Activity Limits

MCG Activity Limits									
Travel		Lodging		Auto Rental		Restaurant		MOTO/EC	
Avail.	Unavail.	Avail.	Unavail.	Avail.	Unavail.	Avail.	Unavail.	Avail.	Unavail.
Risky Purchase		Total Purchase		Total Cash		ATM Cash			
Avail.	Unavail.	Avail.	Unavail.	Avail.	Unavail.	Avail.	Unavail.		

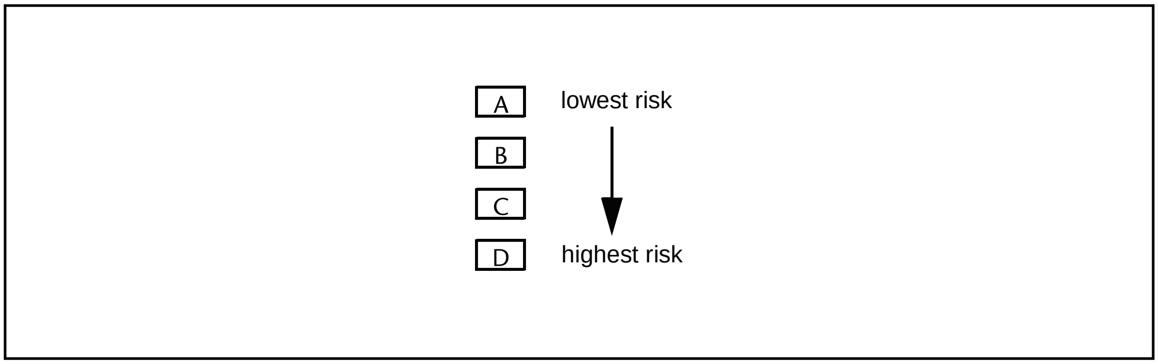
6.7.3 Unique Fields

This subsection describes the unique data fields in the risk-level file.

6.7.3.1 Risk Level

Risk levels allow the issuer to classify an individual cardholder at one of four levels of risk, as shown in Figure 6-1.

Figure 6-1 Cardholder Risk Levels



VisaNet always requires a risk-level classification when an issuer is adding a record to the risk-level file. The V.I.P. default is risk level C if the issuer has specified no other level.

6.7.3.2 Daily Spending Limits

The *daily spending limit* is the maximum whole U.S. dollar amount of cash or non-cash transactions that STIP can approve for the current day.

- Non-cash includes medical, MOTO/EC, risky, and other purchase transactions. VisaNet 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.

6.7.3.3 Merchant Category Group Daily Activity Limits

The *merchant group activity limit* is the maximum whole U.S. dollar 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 dollar 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 *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

6.7.4 Maintenance and Update

Members establish file specifications through their Visa representatives.

6.7.5 Purging Records

Only Visa can purge records in the risk-level file.

6.8 CARD-LEVEL PRODUCT ID

6.8.1 File Description

The *Visa Incentive Network (VIN)* enables issuers to offer highly competitive rewards programs to cardholders. For example, a cardholder receives a 10% 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 Cardholder Database (CDB) with updated information needed for authorization processing. Currently, the VIN provides the CDB with Visa Traditional Rewards program data.

When V.I.P. receives the 0100 authorization or 0200 full financial request from the acquirer, V.I.P. 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, V.I.P. uses the BIN default product value.

6.8.2 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.

Table 6-10 Account-Level Processing (ALP) 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.

6.8.3 Unique Fields

The following fields are unique to the Card-Level Product ID File:

- Activation Date
- Account Product ID
- Rewards Program ID

6.8.3.1 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. V.I.P. 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.

6.8.3.2 Account Product ID

The Product ID is a two-byte field. Currently, the only valid product ID is **B**—Visa Traditional Rewards. Refer to "Field 62.23" in the pertinent BASE I and SMS technical specifications for a full list of product identifiers.

6.8.3.3 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.

6.8.4 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 their Visa representatives.

6.8.5 Purging Records

Issuers provide the purge dates for the file records.

6.9 MERCHANT CENTRAL FILE (MCF)

6.9.1 File Description

The *Merchant Central File Service (MCFS)* augments 0100 authorization requests and 0400 authorization reversals with merchant or terminal identifiers that cannot otherwise be provided. VisaNet stores the augmentation information in the *Merchant Central File*

(MCF). Participating acquirers maintain MCF records. Depending on the record type, augmentation data can include:

- The merchant category code (MCC)
- The terminal identifier
- The merchant name, location, and country
- The province, ZIP, or postal code
- The check acceptance vendor ID
- The merchant verification value (MVV)

In addition to Visa cards, MCFS supports MasterCard, American Express, and Discover cards.

6.9.2 File Content

As shown in the following figure, the MCF organizes records by acquirer institution ID and by merchant identification.

Merchant Central File Record Layout

<table>
<tr><td>Acquiring Institution ID Length</td><td>Acquiring Institution ID</td><td>Merchant Record Type</td><td colspan="7">&lt;---These first fields are common to all Merchant Central File records.</td></tr>
<tr><td colspan="10">Presence of these fields depends on the record type:</td></tr>
<tr><td></td><td>Purge Date</td><td>Merchant ID</td><td>Merchant Type</td><td>Merchant Name, Location, Country</td><td>Terminal ID</td><td>Vendor ID (Reserved)</td><td>Postal Zone</td><td>Update Time</td><td>Effective Time</td></tr>
</table>

Table 6-11 summarizes the fields within a record.

Table 6-11 Merchant Central File Record Fields

Record Type	Record Field	Description	0100/0400 Fields	0300 Fields
Visa, American Express, Check Acceptance, Discover, MasterCard	Acquiring Institution ID Length	Function: key identifier Number of digits in the acquiring institution ID.	Not applicable; resides in the MCF	Not applicable; resides in the MCF
Visa, American Express, Check Acceptance, Discover, MasterCard	Acquiring Institution ID (Acquiring BIN)	Function: key identifier The 4- to 11-digit acquiring institution ID. (It is usually 6 digits.) This field, along with the merchant identification field, constitutes the MCFS file key.	Field 32—Acquiring Institution Identification Code	Field 32—Acquiring Institution Identification Code

Table 6-11 Merchant Central File Record Fields (continued)

Record Type	Record Field	Description	0100/0400 Fields	0300 Fields
Visa, American Express, Check Acceptance, Discover, MasterCard	Merchant Record Type	Function: file maintenance The 1-character code identifying the card program. Valid values are: **A**—Check Acceptance **D**—Discover **M**—MasterCard **V**—Visa **X**—American Express	Not applicable; resides in the MCF	Field 127M.1—Format 2, Merchant Record Type
Visa, American Express, Check Acceptance, Discover, MasterCard	Purge Date	Function: file maintenance The date after which VisaNet removes the record. The format is *MMDDYY*.	Not applicable; resides in the MCF	Field 73—Date, Action
Visa, Universal, American Express, Check Acceptance, Discover, MasterCard	Merchant Identifier	Function: key identifier A unique 1- to 15-digit code for the acquirer BIN's merchant or merchant's terminal. This field, along with the acquiring institution ID, constitutes the MCFS file key. Depending on card type, field 41, field 42, or both, can contain the identifier. In 0300 file update messages, the identifier *to be added, changed, or deleted* is in Field 127M.2—Format 2, Merchant Data 1.	Field 41—Card Acceptor Terminal Identification Field 42—Card Acceptor Identification Code	Field 41—Card Acceptor Terminal Identification Field 42—Card Acceptor Identification Code Field 127M.2—Format 2, Merchant Data 1
Visa, Universal, MasterCard	Merchant Type	Function: augmentation data The 4-digit merchant category code associated with the merchant identifier.	Field 18—Merchant Type	Field 127M.2—Format 2, Merchant Data 1

Table 6-11 Merchant Central File Record Fields (continued)

Record Type	Record Field	Description	0100/0400 Fields	0300 Fields
American Express, Discover	Replacement Terminal ID	Function: augmentation data The 1- to 15-character terminal identification replacement value in field 41 or in field 42 of the authorization request. V.I.P. adds the identifier to the request before STIP-or-issuer routing. V.I.P. reinstates the original value in field 41 or in field 42 of the response.	Field 41—Card Acceptor Terminal Identification Field 42—Card Acceptor Identification Code	Field 127M.2—Format 2, Merchant Data 1
Universal, MasterCard	Card Acceptor Name, Location, Country	Function: augmentation data The 40-digit merchant identifier that comprises a 25-digit card acceptor name, a 13-digit city name, and a 2-digit country code.	Field 43—Card Acceptor Name/Location	Field 127M.3—Format 2, Merchant Data 2 Field 127M.4—Format 2, Merchant Data 2
Universal, MasterCard	Postal Zone	Function: augmentation data An alphanumeric 9-character postal code.	Field 59—National Point-of-Service Geographic Data, positions 6–15	Field 127M.3—Format 2, Merchant Data 2
Universal, Visa	Merchant Verification Value	Function: augmentation data An alphanumeric 10-character MVV code.	Field 62.20—Merchant Verification Value	Field 127M.5, Format 2, Merchant Data 2
Check Acceptance	Vendor ID (reserved)	Function: augmentation data A 1-character alphanumeric code assigned to the vendor. Visa reserves this field for future use.	Field 100—Receiving Institution Identification Code	Field 127M.3—Format 2, Merchant Data 2

6.9.3 Unique Fields

Members decide among the following fields which field BASE I is to use to locate MCFS data for 0100 authorizations and for 0400 reversals:

Field 18—Merchant Type (merchant category code)

Field 41—Card Acceptor Terminal Identification (terminal identification)

Field 42— Card Acceptor Identification Code

Field 43—Card Acceptor Name/Location (merchant name, location, country)

Field 59—National Point-of-Service Geographic Data (province, ZIP, or postal code)

Field 62.20—Merchant Verification Value (MVV)

Field 100—Receiving Institution Identification Code (vendor ID)

Refer to the Merchant Central File Service (MCFS) chapter in *V.I.P. System Services, Volume 2*, for further information about these fields, including update processing and augmentation logic.

6.9.4 Maintenance and Update

Acquirers can update their records by using 0300 online file update messages or by submitting a batch file of updates to the VIC. See "File Maintenance Methods" in this chapter for more maintenance and update information.

6.9.5 Purging Records

Acquirers are responsible for purging their records. See "File Maintenance Methods" in this chapter for more information about file disposition.

6.10 FILE MAINTENANCE METHODS

Issuers can update the Cardholder Database, and acquirers can update the Merchant Central File in any of several ways:

- Using online file update messages for individual updates.
- Transmitting a batch file of updates to the VIC through a VisaNet connection that supports the batch file update function.

NOTE

VisaNet supports batch file updating for the CDB only.

- Using V-SAFE for requests for urgent updates. (This option applies only for updating the Cardholder Database).

Members must establish the controls necessary to ensure the accuracy of the data and the procedures for conveying updates to the VIC.

6.10.1 Online Update Process Summary

Issuer processors can use an online message (0302) to add, to change, or to delete a Cardholder Database record. Acquirer processors updating the Merchant Central File use message type 0300. Members initiate update messages either through the issuer processor computer interface or through their VisaNet connection.

With 0120 and 0322 messages, members can maintain their exception records without having to know the current status of the record on the V.I.P. files. For instance, V.I.P. accepts attempts to add a record for a cardholder that is already in the file as a change request. For more information, refer to "Exception File" in the Cardholder Database chapter in *V.I.P. System Services, Volume 2*.

6.10.1.1 Member Processor Computer Interface

The interface sends updates directly to the VIC or indirectly through a VisaNet connection. V.I.P. 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 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 2, BASE I Messages and Flows.

6.10.1.2 Individual Updates Through VisaNet Connections

Member processors equipped with Direct Exchange (DEX) or a Visa Extended Access Server (EA Server) can send individual updates to the VIC. As with updates from a computer interface, V.I.P. applies terminal updates to the file in real time, and the effective date is the date that the VIC receives the updates. For more information, refer to About This Manual for a list of VisaNet connection and VAP documents.

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.

6.10.1.3 File Maintenance Errors

A file maintenance message that contains errors does not update the file. When V.I.P. returns response code **06** in a file maintenance response, the 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. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for valid reject codes.

All messages must meet the requirements described in *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*.

6.10.2 Batch Update Process Summary

Issuer processors can use batch processing to update cardholder records in the Cardholder Database. The process consists of creating batch files and sending them to the VIC electronically through the issuer's VisaNet connection.

BASE I and SMS issuers can perform a full file replacement for all Exception File records at the BIN level as well as at the Processor Control Record (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 Cardholder Database chapter in *V.I.P. System Services, Volume 2*.

Table 6-12 shows the applicable parameters for the BIN-level full file replacement option.

Table 6-12 Exception File Full File Replacement at BIN Level

	Processing Rules	
File Characteristics	**BASE I**	**SMS**
Media	BASE I issuers may send a file replacement tape electronically to Visa.	SMS issuers may send a file replacement tape electronically to Visa.
File Types	VisaNet permits File types E1 and E2.	VisaNet 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. **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. **NOTE:** *Issuers must right-justify the BIN number and zero-fill the field.*
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: **1** = Replacement of entire file by PCR **2** = Replacement of entire file by BIN **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: **3** = Replacement of entire file by PCR **4** = Replacement of entire file by BIN **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.

6.10.2.1 Batch Updating Through a VisaNet Connection

Member processors equipped with Direct Exchange (DEX) or a Visa Extended Access Server (EA Server) and running the BASE I interface subsystem can send batch files through the VisaNet connection. This method is suitable for large volumes of routine updates. For more information, refer to About This Manual for a list of VisaNet connection and VAP documents.

To use the batch method, member processors first create a tape file. The file can include multiple types of cardholder records such as E2, F2, and so forth. The operator then transfers the file to the VisaNet connection or mounts the tape on the VAP tape drive. When the transfer is complete, the operator transmits the file to the VIC.

V.I.P. applies batch updates sent through VisaNet connections to the files as soon as the VIC receives them. However, unlike individual online updates, the member processor specifies the update effective time in the tape header. VisaNet immediately reports any errors or rejects to the member processor and writes them to a VisaNet connection log.

For batch update records, the file type field (bytes 32–34 in the header record or bytes 1–2 in the detail record) indicates which file the member processor is updating.

For more information about the tape specifications and about the record formats for batch file updates, refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*. For operator instructions related to the VisaNet connection transmission process, see About This Manual for a list of VisaNet connection and VAP documents.

6.10.3 Member Access to File Records

Member processors can request a record at any time while they are signed on to the network, although Visa 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 VisaNet 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 VisaNet. The member processor can also request reports of Advice File and Exception File records.

For Merchant Central File records, the message specifies the merchant identification (merchant ID or merchant terminal ID) and the acquirer processor BIN to be reviewed; the VIC response contains the requested record. For details about online file inquiry requests, refer to the description of message types 0120 and 0322 in Chapter 2, BASE I Messages and Flows, of this manual, and in *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*. Also refer to About This Manual for a list of VisaNet connection and VAP documents.

6.11 ADVICE FILE

6.11.1 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.

6.11.2 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 VisaNet for the following services:
  - Chargeback Reduction Service (T&E chargeback processing)
  - Auto-CDB Service
  - V-SAFE
- 0120 and 0322 discrepancy advices of Exception File update requests that VisaNet 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.

Refer to *V.I.P. System Services, Volume 2*, for the BASE I Advice Retrieval Service description.

6.11.3 Unique Fields

Advices contain specific fields from the original request and response messages. Refer to *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, for details about the fields contained in advice messages.

6.11.4 Maintenance and Update

V.I.P. 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 BASE II.

6.11.5 Purging Records

V.I.P. purges records in the Advice File after issuers recover them or when issuers do not recover them within 15 days.

THIS PAGE INTENTIONALLY LEFT BLANK.

Appendix A

Visa Mandatory Minimum Limits

This appendix contains Visa mandatory minimum (MM) issuer and activity limits.

A.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.

- Chapter 4, BASE I Limits and Routing: This chapter defines issuer limits and describes their use as initial thresholds for routing transactions to issuers or to STIP.
- Chapter 5, 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 card product for a region, it means that the region's mandatory minimum issuer or activity limits do ***not*** apply.

NOTE

The V.I.P. System does not apply mandatory minimum issuer or activity limits to debit or prepaid card transactions.

Table A-1 Visa-Mandated Limit Parameters

					1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
1	**Visa U.S.A. (U.S.)—Domestic**	**Default**[1]	1—Commercial Travel	$250.00	$250.00	$500.00	2	2	3.00	3.00
			2—Lodging	$250.00	$250.00	$500.00	2	2	3.00	2.00
			3—Auto Rental	$250.00	$250.00	$500.00	2	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$500.00	0	2	4.00	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	$0.00	$0.00	0	0	4.00	4.00
			11—Medical	$0.00	$0.00	$500.00	0	2	4.00	2.00

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
					Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
1	U.S.—Domestic	Business Platform non-Signature Scheme	1—Commercial Travel	$400.00	$400.00	$1,000.00	2	2	3.00	3.00
			2—Lodging	$300.00	$300.00	$1,000.00	2	2	3.00	2.00
			3—Auto Rental	$250.00	$250.00	$500.00	2	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$500.00	0	2	4.00	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
1	U.S.—Domestic	Gold Premier Product Id	1—Commercial Travel	$400.00	$400.00	$1000.00	2	2	3.00	3.00
			2—Lodging	$300.00	$300.00	$1,000.00	2	2	3.00	2.00
			3—Auto Rental	$250.00	$250.00	$500.00	2	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.0	4.0
			5—MOTO/EC	$0.00	$0.00	$0.00	0	0	4.0	4.0
			6—Risky Purchase	$0.00	$0.00	$0.00	0	0	4.0	4.0
			7—Other Purchase	$0.00	$0.00	$500.00	0	2	4.00	2.00
			8—Other Cash	$0.00	$0.00	$0.00	0	0	4.00	4.00
			9—ATM Cash	$0.00	$0.00	$200.00	0	1	4.00	4.00
			10—Quasi-Cash	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00

Table A-1 Visa-Mandated Limit Parameters (continued)

					1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
1	U.S.—Domestic	Consumer Platform Electron Scheme	1—Commercial Travel	$0.00	$0.00	$0.00	0	0	4.00	4.00
			2—Lodging	$0.00	$0.00	$0.00	0	0	4.00	4.00
			3—Auto Rental	$0.00	$0.00	$0.00	0	0	4.00	4.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$0.00	0	0	4.00	4.00
			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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
1	U.S.—International	Default [1]	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/EC	$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	$1,000.00	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

Table A-1 Visa-Mandated Limit Parameters (continued)

					1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
1	**U.S.—International**	**Business Platform non-Signature Scheme**	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/EC	$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
			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
1	**U.S.—International**	**Gold Premier Product Id**	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/EC	$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	$200.00	0	1	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

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
					Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
1	U.S.—International	Consumer Platform Electron Scheme	1—Commercial Travel	$0.00	$0.00	$0.00	0	0	4.00	4.00
			2—Lodging	$0.00	$0.00	$0.00	0	0	4.00	4.00
			3—Auto Rental	$0.00	$0.00	$0.00	0	0	4.00	4.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$0.00	0	0	4.00	4.00
			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
2	Visa Canada (CAN)—International	Default[1]	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/EC	$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	$1,000.00	2	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

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
					Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
2	CAN—International	Business Platform non-Signature Scheme	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/EC	$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
			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
2	CAN—International	Gold Premier Product Id	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/EC	$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
			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

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
					Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
3	Visa Europe (VE)—International	Default[1]	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/EC	$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	$1,000.00	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 Platform non-Signature Scheme	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/EC	$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
			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

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
					Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
3	VE—International	Gold Premier Product Id	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/EC	$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
			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
4	Asia-Pacific (AP)—International	Default[1]	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/EC	$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	$1,000.00	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00

Table A-1 Visa-Mandated Limit Parameters (continued)

					1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
4	**AP—International**	**Business Platform non-Signature Scheme**	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/EC	$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
			10—Quasi-Cash	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
4	**AP—International**	**Gold Premier Product Id**	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/EC	$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
			10—Quasi-Cash	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
					Issuer Avail-able (U.S. dollars)	Issuer Unavail-able (U.S. dollars)	Issuer Avail-able	Issuer Un-avail-able	Issuer Avail-able	Issuer Un-avail-able
5	Latin America and Caribbean (LAC)—International	Default[1]	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/EC	$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	$1,000.00	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
5	LAC—International	Business Platform non-Signature Scheme	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/EC	$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
			10—Quasi-Cash	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
					Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
5	LAC—International	Gold Premier Product Id	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/EC	$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
			10—Quasi-Cash	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
6	Central & Eastern Europe, Middle East & Africa (CEMEA)—International	Default[1]	1—Commercial Travel	$0.00	$00.00	$1,100.00	0	2	2.00	2.00
			2—Lodging	$0.00	$0.00	$900.00	0	2	2.00	2.00
			3—Auto Rental	$0.00	$0.00	$600.00	0	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$1,000.00	0	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00

Table A-1 Visa-Mandated Limit Parameters (continued)

					1–Day Activity Limit		1–Day Activity Limit Count		4–Day Activity Limit Multiplier	
Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	Issuer Available (U.S. dollars)	Issuer Unavailable (U.S. dollars)	Issuer Available	Issuer Unavailable	Issuer Available	Issuer Unavailable
6	CEMEA—International	Business Platform non-Signature Scheme	1—Commercial Travel	$0.00	$0.00	$2,200.00	0	2	2.00	2.00
			2—Lodging	$0.00	$0.00	$1,750.00	0	2	2.00	2.00
			3—Auto Rental	$0.00	$0.00	$900.00	0	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$1,750.00	0	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
6	CEMEA—International	Gold Premier Product Id	1—Commercial Travel	$0.00	$0.00	$2,200.00	0	2	2.00	2.00
			2—Lodging	$0.00	$0.00	$1,750.00	0	2	2.00	2.00
			3—Auto Rental	$0.00	$0.00	$900.00	0	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$1,750.00	0	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00

Table A-1 Visa-Mandated Limit Parameters (continued)

Region and Limits Jurisdiction		Product Id Attribute	Merchant Category Group	Issuer Limit (U.S. dollars)	1–Day Activity Limit Issuer Available (U.S. dollars)	1–Day Activity Limit Issuer Unavailable (U.S. dollars)	1–Day Activity Limit Count Issuer Available	1–Day Activity Limit Count Issuer Unavailable	4–Day Activity Limit Multiplier Issuer Available	4–Day Activity Limit Multiplier Issuer Unavailable
6	CEMEA—International	Infinite, Signature Preferred, Infinite Privilege Product Id	1—Commercial Travel	$0.00	$0.00	$2,200.00	0	2	2.00	2.00
			2—Lodging	$0.00	$0.00	$1,750.00	0	2	2.00	2.00
			3—Auto Rental	$0.00	$0.00	$900.00	0	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$1,750.00	0	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00
6	CEMEA—International	Platinum, Visa Rewards, Visa Select Product Id	1—Commercial Travel	$0.00	$0.00	$2,200.00	0	2	2.00	2.00
			2—Lodging	$0.00	$0.00	$1,750.00	0	2	2.00	2.00
			3—Auto Rental	$0.00	$0.00	$900.00	0	2	2.00	2.00
			4—Restaurant	$0.00	$0.00	$0.00	0	0	4.00	4.00
			5—MOTO/EC	$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	$0.00	$1,750.00	0	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	0.00	0.00
			11—Medical	$0.00	n/a	n/a	n/a	n/a	0.00	0.00

[1] No matching Product Id attribute.

Index