Welcome to

V.I.P. System SingleConnect Service SMS Interlink Processing Specifications

This revised manual, which describes Single Message System (SMS) processing for SMS Interlink, contains specific information about processing requirements and options for SingleConnect participants.

This manual contains new information from various sources and reflects SMS changes since September 1996. See the About This Manual chapter for details.

A companion volume, the SingleConnect technical specifications for Interlink, describes message formats, field descriptions, codes, and file specifications. These specifications provide the detailed technical information necessary for SingleConnect issuers and acquirers to implement SMS processing.

The Visa *Confidential* label in the footers indicates the information in this document is intended for use by Visa employees, member banks, and external business partners that have signed a Nondisclosure Agreement (NDA) with Visa. This information is not for public release.

Also included is a questionnaire that allows you to evaluate this manual. Please complete and return the questionnaire to us. You may also write to us at the address printed on the back of the questionnaire or e-mail us at any time. Our e-mail address is buspubs@visa.com. Your opinion is important to us.

Effective: 31 March 2001

SMS Interlink Processing Specifications

SingleConnect Service

V.I.P. System

Effective: 31 March 2001

Printed on recycled paper

Contents

Chapter 3 • Service Participation Requirements

Chapter 4 • Message Types and Flows

Chapter 8 • Routing

Chapter 9 • Settlement and Reconciliation

Figures

Tables

About This Manual

The *V.I.P. System SingleConnect Service SMS Interlink Processing Specifications* manual provides general information about the SingleConnect Service for Interlink. The manual describes processing requirements and options and contains specific information about message types, connectivity, security responsibilities, processing considerations, and related services.

A companion volume, the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*, describes message formats, field descriptions, codes, and file specifications. It provides the detailed technical information necessary for issuers and acquirers to plan the systems development efforts and implement Interlink processing.

Audience

The processing specifications in this manual are intended for technical and systems professionals responsible for implementing the SingleConnect Service for Interlink processing, and for those managing the programs after they are installed.

Organization of This Manual

This manual contains the following chapters:

Chapter 1, Service Overview—Provides a high-level description of the V.I.P. SingleConnect Service and identifies related Interlink features and services.

Chapter 2, SingleConnect Interlink Transactions—Describes the Interlink transactions, transaction sets, and methods for maintaining message integrity.

Chapter 3, Service Participation Requirements—Summarizes the requirements and options for Interlink participants, from both an issuer and acquirer perspective.

Chapter 4, Message Types and Flows—Provides descriptions and message flow diagrams for Interlink transactions.

Chapter 5, Multicurrency Support—Explains how currency conversion is handled.

Chapter 6, Stand-In and Card Verification Value Processing—Provides a detailed description of stand-in and card verification services available to Interlink participants. Additional risk services are also identified, with references to appropriate sources.

Chapter 7, Security—Identifies security responsibilities for Interlink issuers and acquirers. The chapter includes a discussion of PIN usage and security in pertinent transactions.

Chapter 8, Routing—Contains information about Interlink transaction routing and routing tables.

Chapter 9, Settlement and Reconciliation—Contains information on settlement services, daily settlement reports, funds transfer, and the daily settlement schedule.

Chapter 10, Interlink Exception Processing and Dispute Resolution—Contains information about exception processing and dispute resolution for both issuers and acquirers.

Chapter 11, Member-to-Visa Connection Options—Contains information on connectivity requirements and options.

Document Conventions

Table 1 shows the document conventions used in this manual.

Table 1: Document Conventions

Document Convention	Purpose in This Guide
ALL UPPERCASE LETTERS	Drive letters, subdirectory names, file names; system names, statuses, modes, and states.
EXAMPLE	Identifies an example of what the accompanying text describes or explains.
IMPORTANT	Highlights important information in the text.
italics	Document titles; emphasis; variables.
“text in quote marks”	Section names referenced in a chapter.
Note:	Provides more information about the preceding topic.

Documentation Descriptions for Visa International

The first three manuals in this series, *V.I.P. System Overview*, *V.I.P. System Services* and *V.I.P. System Reports*, apply to both BASE I and SMS processing.

There are two manuals specific to the BASE I System: *BASE I Processing Specifications* and *BASE I Technical Specifications*.

There are six manuals specific to the Single Message System: three processing specifications and three technical specifications for ATM, Interlink and POS. Table 2 contains the description of international V.I.P. system manuals.

Table 2: Description of International V.I.P. System Manuals (1 of 3)

General Information	**V.I.P. System Overview** Provides basic descriptions of the VisaNet network and its components, connections, processing concepts, requirements, and options. Contains descriptions of V.I.P., access methods, BASE I and Single Message Systems, issuer and acquirer responsibilities, and Visa Interchange Center operations. Also provides a brief introduction to V.I.P. services. Doc ID 0851-01
	V.I.P. System Reports Provides sample reports for V.I.P. System services, BASE I and Single Message System processing. Doc ID 0852-01
	V.I.P. System Services Provides complete information about V.I.P. System services available for BASE I and SMS users. Service descriptions include basic information, processing requirements, options, features, key message fields, and message flows. Doc ID 0853-01

Table 2: Description of International V.I.P. System Manuals (2 of 3)

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, security responsibilities, related services, and connection options. Doc ID 0847-01
	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. Companion volume to the *V.I.P. System BASE I Processing Specifications* and describes the fields for BASE I. Doc ID 0844A-01
	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. Companion volume to the *V.I.P. System BASE I Processing Specifications* and describes the message formats and file specifications for BASE I. Doc ID 0844B-01
Interlink	**V.I.P. System SingleConnect Service SMS Interlink Processing Specifications** Contains information about Interlink, including message types, processing considerations, connection options, security responsibilities, related services, and reports. Doc ID 0837-02
	V.I.P. System SingleConnect Service SMS Interlink Technical Specifications Companion volume to the *V.I.P. System SingleConnect Service SMS Interlink Processing Specifications*. Describes message formats, field descriptions, and file specifications for Interlink. Doc ID 0838-02

Table 2: Description of International V.I.P. System Manuals (3 of 3)

SMS ATM	**V.I.P. System SingleConnect Service SMS ATM Processing Specifications** Contains information about Single Message System ATM processing, including message types, processing considerations, connection options, security responsibilities, and related services. Doc ID 0839-02
	V.I.P. System SingleConnect Service SMS ATM Technical Specifications Companion volume to the *V.I.P. System SingleConnect Service SMS ATM Processing Specifications*. Contains information about message formats, field descriptions, and file specifications for ATM. Doc ID 0840-02
SMS POS	**V.I.P. System SingleConnect Service SMS POS (Visa & Visa Electron) Processing Specifications** Contains information about Single Message System POS processing, including message types, processing considerations, connection options, security responsibilities, related services, and reports. Doc ID 0835-02
	V.I.P. System SingleConnect Service SMS POS (VISA & VISA Electron) Technical Specifications - Volume 1 Companion volume to the *V.I.P. System SingleConnect Service POS (VISA & Electron) Reference Guide Processing Specifications*. Describes the fields for Visa POS and Visa Electron. Doc ID 0848-01
	V.I.P. System SingleConnect Service SMS POS (VISA & VISA Electron) Technical Specifications - Volume 2 Companion volume to the *V.I.P. System SingleConnect Service POS (VISA & Electron) Reference Guide Processing Specifications*. Describes message formats and file specifications for Visa POS and Visa Electron. Doc ID 0849-01

Sources of Information for These Specifications

This section lists the primary sources for the information contained in the *V.I.P. System SingleConnect Service SMS Interlink Processing Specifications*. The information from these sources has been analyzed, rewritten, and reorganized, when necessary. Technical staff and service experts reviewed and verified these updates. In addition, this new manual incorporates all comments received from members and Visa staff, where appropriate.

Existing Manuals

The following manuals from the existing V.I.P. documentation set were used as sources for the *V.I.P. System SingleConnect Service SMS Interlink Processing Specifications*:

V.I.P. SingleConnect Service Interlink Reference Guide, Processing Specifications

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

Technical Letters

The *V.I.P. System SingleConnect Service SMS Interlink Processing Specifications* includes information from the following technical letters:

September 1996 V.I.P. System Business Enhancements,
Publication DS-9603107, including update bulletins

April 1997 V.I.P. System Business Enhancements,
Publication DS-9609124

September 1997 V.I.P. System Business Enhancements,
Publication DS-9703014, including update bulletins

March 1998 VisaNet Business Enhancements,
Publication DS-9709037

September 1998 VisaNet Business Enhancements,
Publication DS-9803012, including update bulletins

April 1999 VisaNet Business Enhancements,
Publication DS-9810095, including update bulletins

June 2000 VisaNet Business Enhancements,
Publication 4301-01

October 2000 VisaNet Business Enhancements,
Publication 4602-01

Obtaining Report Samples

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

V.I.P. System Reports

VisaNet Settlement Service (VSS) Reference Guide, Volume 2, 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 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.

Related Publications

The publications listed in this section provide information about Visa systems, regulations, and additional services not covered in this manual. Use the following guidelines to receive any of the listed publications, to be added or removed from distribution lists, or to inquire about other publications:

- U.S. members and third-party processors can contact the Visa U.S.A. Member Publications department by sending an e-mail to PUBS@visa.com.
- Members and third-party processors in all other Visa regions can contact their Visa representatives.
- U.S.-based Visa staff (except those in Miami) can send an e-mail request to Docline. Docline distributes VisaNet documentation and attempts to locate other publications distributed elsewhere within Visa.
- Visa staff located outside of the U.S. and in Miami can contact their regional representatives.

To inquire about VisaNet documentation or submit changes and additions, contact VisaNet Technical Publications by sending an e-mail to buspubs@visa.com. Visa staff can send an e-mail to Business Publications.

Operating Regulations

Operating regulations for the six Visa regions are published in the following manuals:

Visa Asia-Pacific Regional Operating Regulations

Visa Canada Regional Operating Regulations

Visa Central and Eastern Europe, Middle East and Africa Regional Operating Regulations

Visa European Union Regional Operating Regulations

Visa International Operating Regulations

Visa Latin America and Caribbean Regional Operating Regulations

Visa U.S.A. Inc. By-Laws and Operating Regulations

For specific information about Interlink bylaws and operating regulations, contact your Visa representative.

V.I.P. SingleConnect Service Documentation

In addition to this manual, Visa provides international members with the following manuals to support SingleConnect processing:

V.I.P. SingleConnect Service Processing Overview—This overview helps new or prospective participants to evaluate the impact of SMS on their systems and operations.

V.I.P. System SingleConnect Service SMS Interlink Technical Specifications—This manual contains detailed technical information about message formats, field descriptions, file specifications, country codes, currency codes, reject codes, and file error codes.

V.I.P. System SingleConnect Service SMS POS (Visa & Visa Electron) Processing Specifications—This manual contains information about SingleConnect support of Visa and Visa Electron POS transactions. It includes information about message types, processing considerations, security responsibilities, related services, and connection options.

V.I.P. System SingleConnect Service SMS POS (Visa & Visa Electron) Technical Specifications—This manual contains detailed technical information about message formats, field descriptions, file specifications, country codes, currency codes, reject codes, and file error codes.

V.I.P. System SingleConnect Service SMS ATM Processing Specifications—This manual contains information about the SingleConnect ATM Service and its support of ATM transactions. It includes information about message types, processing considerations, security responsibilities, related services, and connection options.

V.I.P. System SingleConnect Service SMS ATM Technical Specifications—This manual contains detailed technical information about message formats, field descriptions, file specifications, country codes, currency codes, reject codes, and file error codes.

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

BackOffice Adjustment System (BOAS)

For information on BOAS, refer to the following manuals:

BOAS Administration and Technical Guide

Using BOAS with the BASE II System

Using BOAS with the Single Message System

Risk Management Services

For more information on risk management services, refer to:

Acquirer Bulletin Control Service User's Guide

Card Recovery Bulletin Service User's Guide

Cardholder Risk Identification Service User's Guide

Issuer's Clearinghouse Service PC Mailbox User's Guide

Issuer's Clearinghouse Service User's Manual

Merchant Performance Reporting User's Guide

National Application Review Service User's Guide

National Merchant Alert Service User's Guide

Risk Identification Service User's Manual

Security

For information on data and system security, refer to the following documents:

Card Technology Standards Manual

Consolidated PIN Security Standards Requirements

Single Message System (SMS) Dynamic Key Exchange Service Announcement and Specifications, September 1998

VisaNet Access Points (VAPs)

For information about VAPs, refer to one of the following sets of documentation. The VAP Release 10.23 documentation is for PS/2 architecture. The VAP Release 11 documentation is for PCI and ISA architecture.

VAP Release 10.23 Documentation

VAP Computer Based Training User's Guide

VAP Interface Specifications: BASE II & Other File Processing

VAP Interface Specifications: V.I.P. Processing

VAP Messages & Troubleshooting

VAP Operator's Guide

VAP Software Library

VAP Systems Guide

VAP Release 11 Documentation

VAP Release 11 Interface Specifications: BASE II & Other File Processing

VAP Release 11 Interface Specifications: V.I.P. Processing

VAP Release 11 Maintenance, Messages, & Troubleshooting Guide

VAP Release 11 Operator's Guide

VAP Release 11 Software Library

Miscellaneous Systems and Services

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

Card Verification Value (CVV) Member Implementation Guide

Cardholder Reporting System User's Guide

Visa Image Exchange Workstation (VIEW) User's Guide

V.I.P. SingleConnect Service File Delivery—Direct Access Service (DAS) Technical Specifications

VisaNet Settlement Service (VSS) Reference Guide, Volumes 1 and 2

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

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

VisaNet Test System (VTS) User's Manual

VTS2000 User's Guide

Service Overview 1

The V.I.P. SingleConnect Service allows members worldwide to process POS (point-of-sale and point-of-service) transactions and automated teller machine (ATM) transactions using one connection to VisaNet.

Visa supports the V.I.P. SingleConnect Service for the following cards in all regions (except as noted):

- Cards bearing the Interlink or Visa Interlink mark (Asia-Pacific and U.S. regions only)
- Cards bearing the Plus mark
- Visa cards
- Visa Electron cards

Some non-Visa products are also supported in some countries.

The SingleConnect Service allows an issuer or acquirer to send all VisaNet messages through the Single Message System (SMS). A single connection can be used for authorization, clearing, settlement, exception, and administrative messages.

Understanding the SingleConnect Service requires a basic understanding of VisaNet and the interaction of its system components. This chapter contains information that provides a groundwork for understanding the SingleConnect information in this manual, including:

- A brief description of the VisaNet network and its major systems.
- An overview of SMS message processing and SMS SingleConnect transactions.
- Brief summaries of related services.

A complete overview of VisaNet and the V.I.P. System appears in the *V.I.P. System Overview*.

The VisaNet Network

The V.I.P. SingleConnect Service is available through Visa's Single Message System (SMS), which is a subsystem of VisaNet, the Visa transaction processing network. The term VisaNet applies to all components of the network, from the hardware, software, and communications facilities that connect the Visa network with members' systems and other networks to the systems that perform all transaction processing and system services.

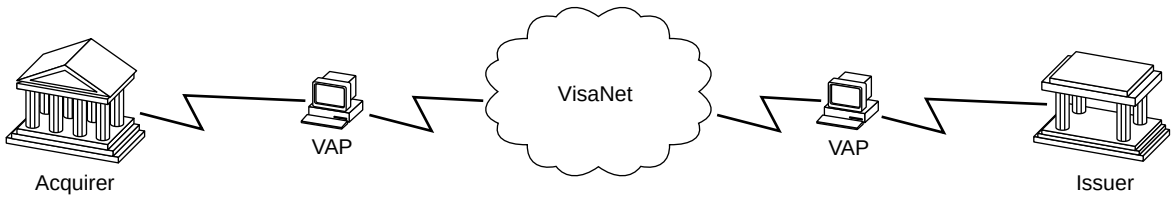
NOTE: *Some readers may have seen online financial processing referred to as single message processing; Visa's preferred terminology distinguishes between the Single Message System and the SingleConnect Service (which is processed through the Single Message System).*

VisaNet routes transactions between acquirers and issuers through its global transaction processing network. Two of the VisaNet processing facilities, OCE and OCW, house SMS as a component of the VisaNet Integrated Payment (V.I.P.) System, Visa's main transaction processing system. Members are connected to VisaNet through VisaNet Access Points (VAPs).

Most acquirers and issuers communicate with the V.I.P. System through a Visa-supplied VAP. Message control and interface functions are performed by the V.I.P. Subsystem in the VAP.

Figure 1–1 illustrates the VisaNet network. SMS is a subset of the V.I.P. System, which is part of VisaNet.

Figure 1–1: The VisaNet Network



VisaNet Systems

The VisaNet network contains two main transaction processing systems.

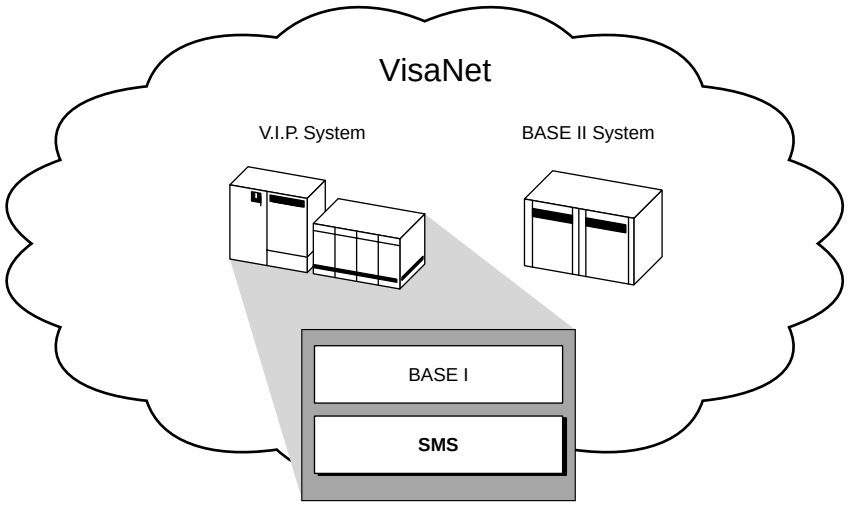
- The VisaNet Integrated Payment (V.I.P.) System, with two components:
  - The Single Message System (SMS), which supports single-message processing.
  - The BASE I System, which supports dual-message processing.

    NOTE: *BASE I is not used in connection with Interlink, which is an SMS product exclusively.*
- The BASE II System, which supports dual-message clearing functions.

  NOTE: *BASE II is not used in connection with Interlink, which is an SMS product exclusively.*

Figure 1–2 shows BASE I and SMS residing within the V.I.P. System, which is part of the VisaNet network, along with BASE II.

Figure 1–2: The VisaNet Software System Components



Visa members and processors may choose to have all of their transactions processed by SMS (through the SingleConnect Service), or use different processing methods for different Visa products.

For example, an issuer can use BASE I and BASE II processing for credit transactions and use SMS processing for debit transactions.

NOTE: *SingleConnect endpoints must use the V.I.P. ISO message format and observe all rules for its use.*

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

The V.I.P. System is the primary online transaction switching and processing system for all authorization and financial request transactions that enter VisaNet. The V.I.P. System provides the Common Interface Function, BASE I, and SMS functionality to members and other users worldwide.

Both the BASE I and SMS components use files of member-supplied cardholder data and processing parameters to perform online processing. Both systems interface to several offline systems, including BASE II and the BackOffice Adjustment System (BOAS).

NOTE: *This manual does not provide details about BOAS. For information about this system, see the "For More Information" section of the About This Manual chapter for a list of BOAS documents.*

The following subsections introduce various access methods and describe the functions of each of the main V.I.P. software components, which are BASE I and SMS.

The Common Member Interface and Other Access Methods

The Common Member Interface (CMI) is an access method that allows V.I.P. members to use the same communication line to send and receive both SMS and BASE I messages.

CMI processing in V.I.P. routes messages to their BASE I or SMS destinations, depending on the type of processing requested, and the processing network in cases where the message specifies a network.

Besides the CMI, other access methods available to V.I.P. members are:

- BASE I only.
- SMS only.

These methods allow members to communicate with only one component of V.I.P.—BASE I or SMS but not both.

Single Message System (SMS)

In the SingleConnect environment, SMS (formerly called Debit) provides single-message authorization and clearing. In addition, SMS supports settlement through the VisaNet Settlement Service (VSS).

Single-message processing uses one message that contains both authorization and clearing information, which are processed simultaneously. Single messages carry all information needed to post a transaction to an account and to enable clearing and settlement. These messages are commonly known as "full financials."

All SingleConnect Service participants are connected to SMS. Only the SMS component performs single-message processing. SMS can also perform *dual-message processing* (that is, an authorization message followed by a clearing and settlement message).

VisaNet, which supports settlement and funds transfer processing for SMS, handles settlement and funds transfer as an automatic follow-up to SMS transaction processing. VSS performs settlement as a separate process that delivers its results through advices and reports. For an illustration of the relationship of VSS to SMS and BASE II, see the "VisaNet Settlement Service (VSS)" section later in this chapter.

In addition to supporting separate processing of authorization and clearing messages, SMS can communicate with BASE I and access outside networks as required to complete transaction processing.

The SMS online functions perform real-time cardholder transaction processing and exception processing. SMS also accumulates reconciliation totals. The SMS offline functions perform activity reporting and pass activity data to VSS. The SMS offline functions also support the delivery of transactions to the BASE II System for members that use dual-message processing.

SMS supports SingleConnect POS (point-of-sale or point-of-service) transactions for the following card products:

- Interlink and Visa Interlink
- Visa and Visa Electron
- Some non-Visa products

SMS supports SingleConnect ATM transactions for the following card products:

- Visa and Visa Electron
- Plus ATM
- Some non-Visa products

For information about ATM processing, refer to the *V.I.P. System SingleConnect Service SMS ATM Processing Specifications*.

The V.I.P. SingleConnect Service can provide quicker settlement and faster clearing, and therefore reduced risk, when compared to traditional BASE I/ BASE II transaction processing. The V.I.P. SingleConnect Service also provides compatibility with some non-Visa networks and other types of transactions that require single-message settlement.

Because SMS processes online full financial transactions in one message format (V.I.P. ISO), SingleConnect participants need to maintain and support only a single system interface. All processing occurs through a single connection to V.I.P.

BASE I System

BASE I provides authorization services for acquirers that use *dual-message processing*.

Dual-message processing uses two separate message cycles to complete a transaction. In the first message cycle, the acquirer submits an authorization request to BASE I. This request contains authorization information. The issuer sends an authorization response message through VisaNet to the acquirer.

In the second message cycle, dual-message acquirers submit a message to BASE II. The second message contains clearing and settlement information for offline processing.

NOTE: *BASE I is not used at all in connection with Interlink, which is an SMS product exclusively.*

BASE II System

BASE II provides dual-message clearing functions. Dual-message acquirers submit second-cycle messages for processing offline by BASE II. Message data is then passed to VSS, which settles with the issuer and acquirer. For more information about VSS, see the "VisaNet Settlement Service (VSS)" section later in this chapter.

The BASE II System clears batch deferred clearing transactions. These are financial transactions that are held by the member, grouped together, and sent as a batch to VisaNet for clearing and settlement processing at a later time. Settlement occurs through VSS.

NOTE: *BASE II is not used in connection with Interlink, which is an SMS product exclusively.*

VisaNet Settlement Service (VSS)

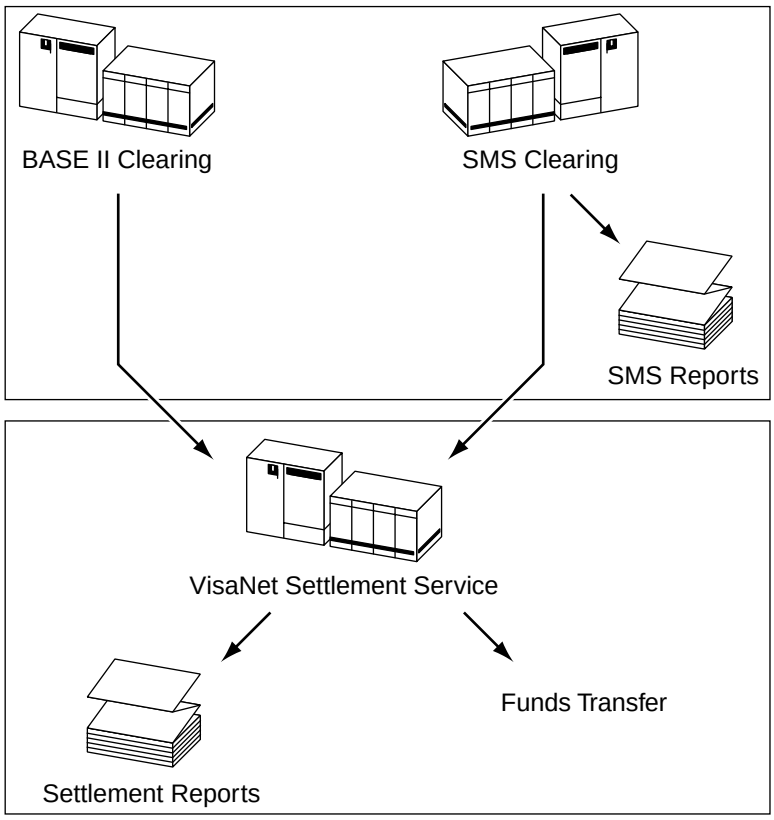
VSS consolidates settlement functions for the Single Message System (SMS) and the BASE II System in one service. Members and processors receive SMS and BASE II settlement information in a standardized set of reports. VSS provides flexibility in defining financial relationships, selecting reports and report destinations, and establishing funds transfer points.

Visa processes interchange transactions for SMS and BASE II through separate systems. Both SMS and BASE II perform their own clearing functions. VSS performs the settlement functions for SMS and BASE II in one centralized service. Clearing and settlement are defined as follows:

- Clearing is the process of collecting an individual transaction from one member or processor and delivering it to another.
- Settlement is the process of calculating and determining the net financial position of each member for all transactions that are cleared.

The VSS clearing and settlement process is shown in Figure 1–3.

Figure 1–3: VisaNet Settlement Service (VSS) Process



SMS Processing Summary

The following describes how a typical online financial SMS transaction flows from the merchant to the issuer and back, what occurs when the issuer system is not available, and what happens at the end of the processing day.

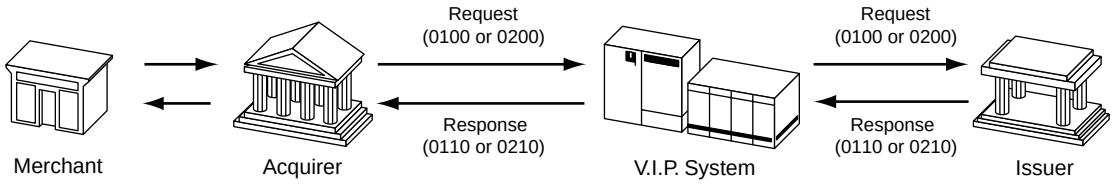
Interlink Online Transaction Flow

Figure 1–4 illustrates how an Interlink online financial transaction is processed.

1. The transaction begins when:
   - A card is swiped through a magnetic-stripe reader.
   - A chip on a card is read by a terminal.

   PINs are required in Interlink transactions and ATM transactions. (PINs are conditional for Visa and Visa Electron cards.)
2. The merchant's acquirer takes the information and creates an 0100 preauthorization or 0200 financial request message, logs the event, and forwards the message to VisaNet.
3. V.I.P. logs and tracks the message, performs any applicable message content editing, initiates service functions such as currency conversion or PIN or CVV verification, and routes the message to the issuer or processes the message in stand-in according to issuer availability and predetermined switching and stand-in-processing (STIP) parameters.
4. The issuer checks the transaction amount against the account's available balance and then checks daily activity limits and other controls, if any. The issuer logs the message and, for approved messages, reduces the cardholder's available balance by the amount of the transaction. The issuer creates an 0110 preauthorization or 0210 financial response message based on the processing results and sends it to VisaNet.
5. V.I.P. logs the response and forwards it to the acquirer.
6. The acquirer logs the financial response and forwards it to the point-of-sale or point-of-service to complete the transaction. The acquirer ensures the response is successfully delivered. If approved, V.I.P. settles the transaction after the next settlement cutoff time.

Figure 1–4: Typical Message Flow



Stand-In Processing (STIP)

Although the SingleConnect POS Service is designed to have transactions authorized online by the issuer, provisions are made to continue processing when the issuer's system is not available due to hardware, software, or communications failure. See Chapter 6, Stand-In and Card Verification Value Processing, for more information about stand-in processing (STIP).

While performing stand-in processing, VisaNet also can verify the Card Verification Value (CVV) to detect the alteration of magnetic stripe data.

The Positive Authorization Capacity Management service (PACM) is used along with STIP to help SingleConnect issuers maximize their authorization and full financial message processing capacity.

PACM monitors the issuer's transaction volume every minute. When the volume of authorization and financial request messages exceeds the issuer's processing capacity, PACM routes low-risk transactions to STIP for the next minute. PACM continues to balance volume with capacity until the issuer is able to process all transactions. PACM creates advices with optional PACM indicators.

End-of-Day Processing

At settlement cutoff, VisaNet determines issuer and acquirer settlement positions and prepares daily reports and raw data files. Raw data files contain detailed information about the day's messages for a given participant. Similarly, issuers and acquirers use their internal transaction logs to account for the day's work and prepare daily reports or files to reconcile to the reports and files from VisaNet. The final step in the settlement process is funds transfer, during which funds are collected from settlement entities with net debit positions and paid to settlement entities with net credit positions.

See Chapter 9, Settlement and Reconciliation, for detailed information about the settlement processes.

VisaNet provides V.I.P. SingleConnect Service participants with a raw data file of all transactions. Members can use this file to match transactions on a one-to-one basis to their systems' records to identify any mismatched transactions and to calculate settlement totals.

Each member's operations staff reconciles data between VisaNet and the member, as well as the sponsored member, processor, or direct-connect merchant. The data from VisaNet is compared against the member's internal transaction data to identify any discrepancies. See Chapter 9, Settlement and Reconciliation, for detailed information.

VisaNet includes a reporting facility that produces daily and monthly reports for issuers and acquirers that subscribe to the V.I.P. SingleConnect Service. The reports fall into two broad categories:

- Transaction detail reports
- Settlement summary reports

Transaction detail reports contain detail about the day's message activity. Each transaction is included on the detail reports including the settlement disposition. Reconciliation totals also are included.

Settlement summary reports contain summary information about the day's work. Totals are provided for the various components including both interchange totals and fee totals.

SMS POS Products for SingleConnect Participants

SingleConnect members can process all of their point-of-sale (POS) transactions through one interface to the Single Message System (SMS). This section summarizes the following SMS POS products:

- Interlink (debit)
- Visa (debit or credit)
- Visa Electron (debit or credit)

NOTE: *The main focus of this manual is Interlink. For Visa and Visa Electron POS processing details, please refer to the* V.I.P. System SingleConnect Service SMS POS (Visa & Visa Electron) Processing Specifications.

Interlink, Visa, and Visa Electron cardholders are allowed to purchase goods and services at participating merchant locations. To support these POS transactions, a member bank has an option to participate in SingleConnect as an issuer, as an acquirer, or as both an issuer and acquirer.

In the online financial environment, a single exchange of messages between the acquirer (or direct-connect merchant) and the issuer is used to:

- Authorize a financial transaction.
- Post a financial transaction to the cardholder's account.
- Post a financial transaction to the merchant's account.
- Clear funds between the acquirer and issuer.

The purchase exchange consists of a request message from the acquirer, followed by a response from the issuer.

SMS POS Products for Acquirers

SMS allows SingleConnect acquirers to consistently process Visa, Visa Electron, and Interlink transactions for their merchants. If a member participates in multiple POS services, SingleConnect acquirers can use one message format and one connection to the SMS component of VisaNet. They also can use the same connection to support their SMS ATM services.

SingleConnect POS acquirers can process a financial transaction in two ways:

- They can authorize and clear POS transactions by submitting a single online financial message to VisaNet. This function occurs when the final purchase amount is known at the time of authorization.
- They can authorize transactions online and submit an online financial message through VisaNet at a later time. This function occurs when the final purchase amount is not known at the time of authorization. This method of processing differs depending upon the POS card program:
  - Interlink acquirers can preauthorize Interlink transactions and submit an online financial message through VisaNet within two hours. The Interlink preauthorization transaction is an online financial transaction set that involves a preauthorization transaction followed by a second clearing, or completion, transaction.
  - Visa and Visa Electron POS acquirers can use online deferred clearing processing.

Acquirers serve as the points of interaction between the merchants and VisaNet. Acquirers are required to:

- Support the acquirer transaction set. (See Chapter 3, Service Participation Requirements, for a list of transactions that acquirers are required to support.)
- Log all financial and nonfinancial transactions (approved or declined) and all postings to merchant accounts.
- Forward responses to the POS device and determine successful delivery of responses.
- Assure total system security of cardholders' PINs. PIN usage is required for Interlink but conditional for Visa and Visa Electron cards. See Chapter 7, Security, for information about PIN security and conditional usage.
- Process exception transactions (initiate adjustments and representments and receive chargebacks).
- Send and receive administrative messages.

SMS POS Products for Issuers

Participating SingleConnect issuers can process Interlink, Visa, and Visa Electron POS transactions using one message format and one connection to the SMS component of the V.I.P. System. They also can use the same connection to support their SMS ATM Services.

V.I.P. SingleConnect POS issuers can immediately authorize and post online financial transactions received from SingleConnect POS acquirers.

In addition, Visa and Visa Electron issuers must be able to authorize transactions online at the time of purchase and receive online deferred clearing transactions through the V.I.P. System at a later time.

Similarly, Interlink issuers must be able to preauthorize transactions online and receive preauthorization completion transactions through SMS at a later time. (See Chapter 4, Message Types and Flows, for more information about processing preauthorizations and preauthorization completions.)

In both cases, the authorization and clearing messages are delivered through the issuer's SingleConnect interface, enabling the issuer to maintain one consistent method for processing preauthorization and preauthorization completions.

The main function of issuers' systems is to respond accurately (based on cardholders' accounts and PINs) to messages received from the V.I.P. System. Issuers also must send chargebacks, administrative messages, and network management messages. Issuers receive transaction requests and approve or decline them based on predefined parameters.

Issuers are required to:

- Support the full complement of Interlink transactions. (See Chapter 3, Service Participation Requirements, for a list of transactions that issuers are required to support.)
- Approve or decline all financial transaction requests.
- Receive advices from the stand-in processor.
- Log all transactions.
- Initiate chargebacks and receive adjustments and representments.
- Send and receive administrative messages.

Available Services

This section identifies the SMS services available to SingleConnect Interlink participants.

Routing Services

Routing refers to decisions relating to sending transactions from the acquirer to VisaNet, and from VisaNet to the issuer. As a rule, Visa assumes responsibility for routing a request to its proper destination. Acquirers do not have to determine how the transaction will be routed to the issuer.

Visa provides a variety of routing services that enable issuers and acquirers to route their transactions precisely as they specify. Most of the routing services that Visa provides are optional. Issuers can designate an alternate path for routing particular transaction types. For example, POS transactions can be routed differently than ATM transactions; exception transactions can be routed differently than authorizations and financial transactions.

Priority Routing Service

This service enables acquirers that accept more than one card brand (or mark) to assign each of them a priority. Prioritization allows V.I.P. to determine the actual network and set of program rules to use for each transaction.

Another use for Priority Routing is to prioritize non-Visa programs destined for VisaNet's gateways to other systems and networks provided by Gateway Services. Refer to Chapter 8, Routing, for more information about this service.

Alternate Routing

This service allows acquirers and issuers to choose separate routing for certain transaction types, including exception items and other back office transactions. Issuers and acquirers may designate their primary processing center to process online original transactions and one or more alternate processing centers to process exception and back office transactions.

Refer to Chapter 8, Routing, for more information about this service.

Authorization Services

Visa offers the following authorization services that can be used by Interlink participants.

Card Verification Value Service

The Card Verification Value (CVV) Service protects issuers and acquirers from fraud losses associated with counterfeit Visa cards. The CVV Service allows issuers to detect invalid cards by checking the content on the magnetic stripe of the cards.

The CVV is a unique value calculated from the data encoded in the magnetic stripe using a Data Encryption Standard (DES) algorithm established by Visa. The issuer or the V.I.P. stand-in processor (STIP) can perform CVV calculation before V.I.P. forwards the transaction to the issuer's processor.

NOTE: *CVV refers to the value encoded on the card; the CVV Service refers to the Visa verification service available through the V.I.P. System.*

The CVV Service depends upon acquirers providing complete, unaltered magnetic stripe data in 0100 preauthorization messages and 0200 financial messages. V.I.P. or the issuer cannot perform CVV calculation when either the issuer or acquirer is not participating in the service or if the magnetic stripe was not read.

For details about this service, refer to Chapter 6, Stand-In and Card Verification Value Processing.

Card Verification Value 2 Service

The Card Verification Value 2 (CVV2) Service is a card verification tool designed to reduce fraud losses when the card is not present. Issuers can imprint a 3-digit security number (the CVV2) on the back of Interlink cards, in accordance with applicable operating regulations.

Although a CVV2 value is never passed in Interlink transactions, Interlink cards can carry a CVV2 number for purposes of card activation, address changes, voice response unit (VRU) cardholder validation, and other bank customer service options to ensure that the cardholder has the "real" card in hand.

PIN Verification Service

The PIN Verification Service (PVS) provides full-time or stand-in verification of personal identification numbers (PINs) used for Interlink transactions, ATM transactions, and any Visa or Visa Electron transactions requiring a PIN. A *personal identification number* is a secret code that identifies a cardholder at a terminal or ATM. A PIN serves as an electronic substitute for a cardholder's signature.

At the issuer's option, the V.I.P. System can verify PINs on behalf of the issuer center at all times or only when the center is unavailable. When V.I.P. verifies PINs, it intercepts all authorization requests containing PINs, verifies the PINs, and passes the requests to the issuers or the V.I.P. stand-in processor (STIP), as appropriate, for authorization processing.

Participation in PVS is optional. For a full description of PVS, see *V.I.P. System Services*. For more information on PIN security, refer to Chapter 7, Security.

Dynamic Key Exchange Service

The Dynamic Key Exchange (DKE) Service is an optional service that enables SingleConnect members to change Data Encryption Standard (DES) cryptographic keys with Visa through the use of online messages.

Working keys are used to encrypt and de-encrypt customer PINs when they are transmitted between the SingleConnect participant and VisaNet. An SMS service participant can periodically change acquirer or issuer or both working keys by exchanging online messages with VisaNet. Two options are available:

- A participant can request new working keys at any time.
- A participant can request in advance that VisaNet automatically create new working keys on a daily basis.

To ensure that the participant and VisaNet are using the same keys, the participant must acknowledge successful receipt of a new key.

For details about this service, refer to Chapter 7, Security.

Additional Services

This section includes additional services available to Interlink members.

Multicurrency Service

The VisaNet Multicurrency Service supports authorization, clearing, and settlement processing in international currencies.

For details, refer to Chapter 5, Multicurrency Support.

SMS Advice Retrieval Service

The SMS Advice Retrieval Service enables issuers to use online connections to recover all types of advices from the SMS Advice File. Such advices are used to communicate information related to STIP, funds transfer, fee collections/ disbursements, and so on.

For more information about this service, refer to the advice recovery sections in Chapter 4, Message Types and Flows, and Chapter 6, Stand-In and Card Verification Value Processing.

Fees and Charges

Fees and charges for the V.I.P. SingleConnect Service are collected either daily through the daily settlement process or monthly through Visa's monthly billing process.

Member-to-Member Fees

A fee is a vehicle for passing costs between members. An *interchange reimbursement fee* (IRF) is an example of a fee. Fees are paid either by the acquirer to the issuer or by the issuer to the acquirer.

Interchange Reimbursement Fees (IRFs)

There are three types of IRFs:

- Domestic Interchange Reimbursement Fees—Fees paid by one participant to another for transactions acquired and issued in the same country.
- Intraregional Interchange Reimbursement Fees—Fees paid by one participant to another for transactions acquired and issued in different countries of the same Visa region.
- Interregional Interchange Reimbursement Fees—Fees paid by one participant to another for transactions acquired and issued in different Visa regions.

In this context, transaction country is the country in which the transaction takes place, and issuing country is the country of the issuer of the card used in the transaction.

If no domestic IRF has been established, the intraregional IRF applies. If no intraregional IRF has been established, the interregional (international) IRF applies.

IRFs are settled daily through the settlement process.

For POS transactions, IRFs are typically paid by acquirers to issuers. Fees for manual cash disbursements, reversals, POS cancellations, merchandise returns, chargebacks, and credit adjustments flow in the opposite direction.

Fees Assessed by Visa

Some fees are passed between a member and Visa.

Currency Conversion Fees

Currency conversion fees are assessed by Visa when the transaction currency (currency used at the point of transaction) and the issuer's cardholder billing currency (currency posted to the cardholder's account) are different. The fees are assessed and settled daily.

See Chapter 5, Multicurrency Support, for more information on currency conversion.

Charges Assessed by Visa

A charge is a vehicle used to bill members for Visa processing costs. There are *single transaction charges* and *service charges*. A charge can be issuer- or acquirer-unique or it can apply to both members. The charge paid by the member is credited to the member's Visa region. Charging requirements vary by region and are subject to approval by the regional board. Each region establishes the specific criteria by which its charges are assessed.

Processing Charges

Transaction switching charges are assessed by Visa both to issuers and acquirers for transactions processed through VisaNet. These charges, which may vary by transaction type, are billed monthly.

Administrative and Service Charges

Administrative and service charges include:

- Cardholder Database Residency Charges—These fees are for items maintained on the Exception File, the PIN Verification File, and the Address Verification File.
- Cardholder Database File Update Charges—These fees are for updates made to the Exception File, the PIN Verification File, and the Address Verification File.
- Access and Use Fees—These fees are for Visa direct-connect members and processors.
- Settlement and Reconciliation Charges—These fees are for additional funds transfers over and above the single transfer per VisaNet endpoint per day, which can be made at no charge.

Most administrative and service charges are billed monthly.

See the applicable Visa operating regulations for detailed descriptions of fees and charges.

Reporting Fees and Charges

Visa reports fees and charges on both a daily and monthly basis. V.I.P. SingleConnect Service charges are passed by the individual transaction processing systems to the Integrated Billing System (IBS), which consolidates them for reporting to members. Visa also reports administrative and service charges, such as monthly VAP access charges. Transaction charges are accumulated daily and billed monthly. Charges that have been settled by other Visa systems are included in the reports to provide a complete accounting of Visa charges for the member. IBS reports are produced monthly.

Daily Fee Reporting

Reimbursement fees and currency conversion fees are listed on the daily reconciliation summary reports. Fees and charges assessed by Visa are reported on the daily settlement reports.

Monthly Reporting and the Integrated Billing System (IBS)

Processing charges reported monthly include administrative and service charges. IBS reports are produced monthly, and include accumulated daily charges.

The IBS reports all member-to-Visa charges on a monthly basis, accumulating daily charges for this billing. Categories that are reported include:

- Processing charges.
- Administrative and service charges.

Visa Integrated Billing Statement

Every SMS participant receives a Visa Integrated Billing Statement, which is produced monthly to give members a unified picture of the Visa products and services they use. Charges for authorization, clearing and settlement, single-message processing, and all other Visa services are reported in the statement. All single message processing and administrative charges are listed on the statement, including those collected through the daily settlement process.

SingleConnect Interlink Transactions 2

This chapter identifies the transactions supported for Interlink (and the other SMS POS products), gives a brief description of each Interlink transaction type, and explains how SMS participants maintain message integrity for all transactions.

Transaction Types

Table 2–1 lists the transaction types supported by SMS for Interlink, Visa POS, and Visa Electron.

Table 2–1: SMS Transaction Types (1 of 3)

Transaction Type	Message Type	Visa POS	Visa Electron	Interlink
Cardholder Transactions				
Preauthorization	0100			✔
Authorization	0100	✔	✔	
Manual or ATM Cash Disbursement	0200	✔	✔	
Account Transfer	0200			
Purchase	0200	✔	✔	✔
Purchase with Cashback	0200			✔
Quasi-Cash	0200	✔	✔	
Key-Entered Purchase	0200	✔	✔	
Scrip	0200			✔
Purchase with Address Verification	0200	✔		

Table 2–1: SMS Transaction Types (2 of 3)

Transaction Type	Message Type	Visa POS	Visa Electron	Interlink
Deferred Clearing Purchase	0220	✔	✔	
Preauthorization Completion	0200			✔
Merchandise Return or Credit	0200	✔	✔	✔
POS Cancellation	0200			✔
Interlink Balance Inquiry	0200			✔
ATM Balance Inquiry	0200	✔	✔	
Address Verification Only	0100	✔		
Merchant-Authorized Transactions				
Store-and-Forward	0200			✔
Paper Sales Draft (Online Financial); (can be submitted using BOAS but not delivered to BOAS destination)	0200			✔
Resubmissions	0200			✔
System-Generated Transactions				
Reversal or Preauthorization Reversal	0400/0420	✔	✔	✔
Exception Transactions (can be submitted using BOAS)				
Adjustment	0220	✔	✔	✔
Chargeback	0422	✔	✔	✔
Chargeback Reversal	0422	✔	✔	
Representment	0220	✔	✔	✔
Fee-Related Transactions				
Acquirer-Generated Fee Collection/Funds Disbursement	0220	✔	✔	
Issuer-Generated Fee Collection/Funds Disbursement	0422	✔	✔	
Reconciliation Transactions	0500/0520	✔	✔	✔
File Maintenance Transactions				
Online File Maintenance	0302	✔		✔
Automatic Cardholder Database Update (Auto-CDB)	0322	✔		

Table 2–1: SMS Transaction Types (3 of 3)

Transaction Type	Message Type	Visa POS	Visa Electron	Interlink
Administrative Transactions				
Free Text Message	0600	✔	✔	✔
Copy Request/Confirmation	0600	✔	✔	
VCRFS Copy Request, Copy Fulfillment, Nonfulfillment, or Dispute	0600	✔	✔	
VCRFS Dispute Ruling	0620	✔	✔	
Funds Transfer	0620	✔	✔	✔
CRIS Alerts	0620	✔	✔	
Online Fraud Reporting	9620	✔	✔	
Network Management Transactions	0800	✔	✔	✔

Interlink Cardholder Transactions

SMS supports the following cardholder transactions for Interlink.

Preauthorization and Preauthorization Completion—This transaction is designed for merchant locations, such as fuel pumps, where the purchase amount is not known at the time the transaction is initiated, but the final transaction amount can be provided within two hours. Preauthorizations consist of an initial request message containing an estimated purchase amount followed by a completion message.

The merchant is guaranteed payment if:

- The preauthorization completion message is received within two hours of the corresponding preauthorization request message.
- The amount in the completion message does not exceed the amount approved by the issuer.

Issuers can send a partial amount response to a preauthorization request when the full amount of a preauthorization request would exceed the cardholder's available funds or daily spending limit, but a lower amount could be approved.

Purchase—The purchase transaction is the basic POS transaction used for Interlink processing. Variations of the purchase transaction include:

- Purchase with cashback.
- Scrip.

Purchase With Cashback—Cashback is a variation of the purchase transaction that permits the cardholder to get cash in addition to goods or services.

Scrip—Scrip is a paper receipt that can be exchanged by the bearer for goods or services combined with cash, as specified by the merchant. These transactions are used by U.S. merchants with self-service terminals that dispense scrip. Scrip transactions are available only for Interlink acquirers in the U.S. region. Scrip transactions must be supported by Interlink issuers outside the U.S. region for the convenience of their cardholders when they are in the U.S. region, but they are not offered to acquirers outside the United States.

Merchandise Credit—A merchandise credit transaction enables merchants to credit the account of an Interlink cardholder who returns merchandise.

POS Cancellation—This transaction is used at the point of sale to cancel a completed financial transaction (purchase or merchandise credit). POS cancellations can be initiated by a merchant or the cardholder at the time of the purchase if a transaction was approved by the issuer but is incomplete or incorrect (for example, if the amount is wrong). Three conditions apply:

- The POS cancellation must be initiated on the same day the transaction being cancelled occurred.
- The cancellation must be performed at the same merchant location at which the original transaction occurs.
- The cardholder and card must be present so that the card can be read electronically and the PIN can be entered.

Balance Inquiry—Balance inquiry transactions allow cardholders to check their balances at stand-alone merchant terminals away from the point of sale.

If the issuer system cannot be reached, VisaNet stand-in processing responds that the issuer is not available. If the issuer is available and supports balance inquiries, the account balance is returned to the acquirer for display or printing in the currency of the merchant.

Merchant-Authorized Transactions

Store-and-forward and paper sales draft transactions are used by Interlink merchants by prior arrangement with the acquirer when the merchant systems are down or unable to communicate with the acquirer. These

transactions must be processed within nine calendar days following the date of the original transactions. Neither the issuer nor Visa is liable for any losses resulting from merchant-authorized transactions, nor is the merchant guaranteed payment for them.

Store-and-Forward—Store-and-forward transactions are completed purchase and merchandise credit transactions that are created and retained by the merchant system when it is not able to submit financial transactions for approval. Later, when the merchant system is back online, the merchant sends the store-and-forward transactions to VisaNet for delivery to the issuers for approval.

Paper Sales Draft—Paper sales draft transactions can be used by merchants when temporary problems occur at the POS terminal or PIN pad. For this transaction the merchant gets the cardholder's signature on the paper sales draft and verifies the cardholder's identity. Later, the merchant forwards the paper sales drafts to the acquirers for conversion to electronic form. The acquirers then submit the electronic sales draft transactions online through VisaNet to the issuers for approval.

Resubmissions—A resubmission is used by acquirers to resubmit a financial transaction (such as an original purchase, store-and-forward, or paper sales draft) that was declined because of insufficient funds or because the transaction would have caused daily activity limits to be exceeded.

For example, a merchant may elect to complete a declined transaction for a regular customer (even though the issuer declined the transaction because of daily limits) with the expectation that the transaction will be approved when resubmitted the next day.

Transactions can be resubmitted once a day for nine calendar days following the date of the cardholder's transaction (not the date of the denial). The resubmission transaction message does not include the PIN, but does include tracing or tracking data that identifies the previously declined transaction.

Merchant systems also can resubmit a store-and-forward transaction after the original store-and-forward transaction is declined for funds-related reasons. Acquirers can resubmit paper sales drafts if the original paper sales draft is declined for funds-related reasons.

System-Generated Transactions

The following subsections describe system-generated transactions that SMS supports for Interlink.

Reversals

A reversal transaction can be initiated by an acquirer's host system or by V.I.P. In contrast to an Interlink POS cancellation, which is initiated by the cardholder or by merchant personnel, a reversal transaction is system-generated.

Issuers and acquirers must match reversals to the corresponding preauthorizations or financial transactions by using tracing data, as discussed in the "Message Integrity" section of this chapter.

There are two types of reversal transactions: *reversal requests* and *reversal advices*. Visa prefers reversal advices. Both transactions must occur on the same calendar day as the transaction being reversed.

Member-Generated Reversals—POS acquirers and merchants use reversals, which are automatically generated by the member's system, to reverse approved authorizations or financial transactions that were not completed due to system malfunctions or because the transactions timed out. Financial transactions are:

- Purchases.
- Interlink credit returns.
- Interlink POS cancellations, including store-and-forward transactions, paper sales drafts, and resubmissions.

POS reversals can be used by:

- A merchant, to reverse a preauthorization when the cardholder does not complete a purchase.
- A merchant, to reverse any previous request when the response is not received at the POS or is received late.
- An acquirer, to reverse a prior request when the acquirer's system did not receive a response, received a late response, or is unable to forward an approval response to the POS.
- An acquirer, when a communications failure prevents transmission of a reversal request. The acquirer's system stores the reversal and forwards it to VisaNet when communications are restored.

V.I.P.-Generated Reversals—V.I.P. generates reversal advices in the following circumstances:

- When a reversal cannot be forwarded to an issuer. In this case, V.I.P. responds to the acquirer and stores a reversal advice for later delivery to the issuer.
- When an approval response cannot be delivered to an acquirer. In this case, V.I.P. generates a reversal request for the issuer and a reversal advice for the acquirer.

Exception Transactions

The following transactions are used to correct errors that occur at the point of transaction or in a participant's system:

- Adjustment
- Chargeback
- Representment

Issuer systems must be able to create chargebacks and receive adjustments and representments. Acquirer systems must be able to receive chargebacks and create adjustments and representments.

Adjustment—An acquirer initiates an adjustment to the cardholder's account for an original transaction in order to correct an error, such as an out-of-balance condition at the POS. The adjustment can be either a debit or a credit (because the cardholder's account was charged either less or more than the actual amount agreed on at the time of the transaction).

Good faith collections are used when an adjustment is required outside of the time frames designated in the operating regulations.

Chargeback—A chargeback transaction is used to credit a cardholder's account for the purchase amount under certain conditions.

An issuer can initiate a chargeback when:

- A cardholder disputes a transaction.
- A cardholder asserts that merchandise was returned, but a merchandise credit transaction has not been received by the issuer.
- The issuer itself disputes a transaction.
- The issuer receives an unpostable debit adjustment from an acquirer.

Representment—Acquirers can initiate a representment transaction message to debit a cardholder's account when the validity of a chargeback can be disproved.

A representment is for the amount of the chargeback, but the chargeback may have been for a partial amount (less than the original amount).

Reconciliation Transactions

VisaNet uses reconciliation transactions to provide cumulative financial totals to issuers and acquirers when requested and at the end of the day. These reconciliation totals are used by SingleConnect participants to verify processing totals throughout the day. Receipt of reconciliation messages is optional for issuers and acquirers.

Members can initiate an online message at any time to receive the previous day's end-of-day totals or current reconciliation totals.

File Maintenance Transactions

File maintenance transactions are used by Interlink issuers that subscribe to one or more of the following optional services:

- PIN Verification Service
- Exception File Service

There are two types of file maintenance transactions:

- File Update—This transaction is used to update the issuer's entries on the PIN Verification File or the Exception File.
- File Inquiry—This transaction is used to review the issuer's entries on the PIN Verification File or the Exception File.

File maintenance transactions can be submitted as individual messages or in batch mode.

For details about online file maintenance messages, refer to Chapter 4, Message Types and Flows, and appropriate V.I.P. System technical specifications.

For details about batch file maintenance, see the "Files" appendix of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications.*

Administrative Transactions

Administrative messages, which are initiated by an SMS participant's operations staff, are used to request or convey information between participants.

SMS administrative messages consist of:

- Free Text Messages—These messages are used to provide or request information of a general nature for POS transactions. Because these messages contain free-text, rather than codes, they can be routed to a printer, for manual evaluation, or documented on a report.

  Administrative free text messages must be supported by all issuers and acquirers.

- Funds Transfer—These messages are used to send the day's final funds transfer totals after completion of settlement and reconciliation.

Network Management Transactions

SMS POS acquirers and issuers must support all network management transactions, except the reconciliation request and the dynamic key exchange, which are optional.

Network management transactions are used to perform the following functions:

- Sign-On—Issuers and acquirers use this function to notify VisaNet that they are available to send and receive messages.
- Sign-Off—Issuers and acquirers use this function to notify VisaNet that they are not available.
- Recovery Sign-On—Issuers and acquirers use this function to request delivery of advice messages.
- Recovery Sign-Off—Issuers and acquirers use this function to indicate that they do not want to receive advice messages.
- Reconciliation Request—Issuers and acquirers use this function to request the current or previous day's processing totals.
- Echo Test—Issuers, acquirers, and VisaNet use this function to confirm the availability of the communications link between the member's host system and VisaNet.
- Dynamic Key Exchange—Issuers, acquirers, and VisaNet use this function to update working keys online. See Chapter 7, Security, for information about keys.

Transaction Sets

VisaNet uses transaction sets to manage all authorizations and financial messages. A transaction set consists of related messages. It enables the acquirer to establish relationships between messages and allows VisaNet and the issuer to identify those relationships. A transaction set provides all three parties with the controls needed for real-time account posting and for updating settlement accumulators.

A transaction set consists of one or more transactions. A transaction consists of one or more system transactions. A system transaction is a pair of messages: a request and response, or an advice and advice response.

Within a given transaction set, SMS allows only certain transactions, and within a given transaction, SMS allows only certain system transactions.

Interlink Transaction Sets

Interlink transaction sets consist of the following:

- Purchase
- Preauthorization
- Merchandise credit
- Balance inquiry
- Paper sales draft
- Store-and-forward
- Resubmission

The following tables, beginning with Table 2–2 and ending with Table 2–7, show the valid Interlink transaction sets, and within each set, the allowable transactions and valid system transactions. System transactions are, from left to right, the original request, reversal, chargeback, and representment.

These tables show all transactions permitted in a transaction set, not those that would be present for a typical transaction set. If a transaction completes satisfactorily under normal conditions, the set contains only the original submission. An exception is a preauthorization, which would include a preauthorization request and preauthorization completion.

Table 2–2: Purchase Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Representment
Purchase	✔	✔	✔	✔
Resubmission	✔	✔	✔	✔
POS Cancellation	✔		✔[1]	✔[1]
Adjustment	✔		✔	✔

[1] Chargebacks and representments are always tied to the original purchase transaction.

Table 2–3: Preauthorization Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Representment
Preauthorization Request	✔	✔		
Preauthorization Completion	✔	✔	✔	✔
POS Cancellation	✔		✔[1]	✔[1]
Adjustment	✔		✔	✔

[1] Chargebacks and representments are always tied to the original purchase transaction.

Table 2–4: Store-and-Forward Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Representment
Store-and-Forward (Purchase or Merchandise Credit)	✔	✔	✔	✔
Resubmission	✔	✔	✔	✔
Adjustment	✔		✔	✔

Table 2–5: Paper Sales Draft Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Representment
Paper Sales Draft (Purchase)	✔	✔	✔	✔
Resubmission	✔	✔	✔	✔
Adjustment	✔		✔	✔

Table 2–6: Merchandise Credit Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Representment
Merchandise Credit	✔	✔	✔[1]	✔[1]
POS Cancellation	✔		✔[1]	✔[1]
Adjustment	✔		✔	✔

[1] Chargebacks and representments are always tied to the original purchase transaction.

Table 2–7: Balance Inquiry Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Representment
Balance Inquiry	✔			

Message Integrity

Maintaining message integrity is a basic requirement of V.I.P. SMS processing. Message integrity assures V.I.P. SingleConnect participants that all other participants have followed the rules, and that a participant can act on a message or transaction as defined—for example, a completed transaction was actually completed and a cancelled transaction was, in fact, cancelled.

Ensuring message integrity requires that all participants keep track of incoming and outgoing messages and generate reversals for transactions that cannot be completed. This process involves concepts of transaction tracing, transaction control, and transaction sets.

Transaction tracing can be accomplished by using the message type and one or more other key data elements to match request and response messages; to match reversals to original transactions; and to tie a transaction, such as a chargeback, to the original transaction.

Key data elements include:

- Transmission date and time.
- Systems trace audit number.
- Acquiring institution ID.
- Retrieval reference number.
- Original data elements.

The acquirer must use messages that are consistent for a transaction set. SMS enforces these rules by comparing an incoming message with previous messages containing the same key data elements. In general, SMS rejects any message that is out of context or out of sequence.

SMS performs consistency editing to prevent invalid, out-of-context messages from being sent to an issuer.

Message Validity

A transaction set cannot include invalid transactions. For example, a purchase transaction set cannot include a balance inquiry or a merchandise return.

A transaction cannot be processed with invalid system transactions. For example, a preauthorization cannot be charged back or re-presented.

In addition, the function of a response must correspond to the function of the request. For example, a reversal response to a purchase request is not valid.

Transaction Sequence

Within a transaction set, transactions must be processed in a logical sequence. For example, in a purchase or merchandise return transaction set containing an adjustment, the original purchase or merchandise return must precede the adjustment.

Account Number Consistency

Within a transaction set, all messages requiring an account number must contain the same account number. If the first message in a transaction set contains an account number, the same account number must be used in all subsequent messages that require an account number.

Amount Consistency

The value in Field 4—Amount, Transaction must be identical in all request/response pairs that require an amount, except in an Interlink preauthorization response, whose value in a partial approval can be less than the amount requested.

All transactions within a transaction set must contain the same transaction amount except for:

- Chargebacks, representments, and adjustments.
- Preauthorization completion advices, whose amounts can be less than the amount approved because partial approvals are allowed.

Representments of transactions must be for the same amount as the original transaction or chargeback.

Processing Duplicate Messages

A duplicate message has the same message type and key data elements (Acquiring Institution ID, Retrieval Reference Number, Trace Number, Transmission Date and Time, and Transaction Identifier) as a prior message. SMS processes duplicates as follows:

- If processing of the original request was completed (a response was sent), SMS responds to the acquirer with a response code of “94” (duplicate transmission) in field 39 and, optionally, includes the original response value in field 44.11. In this case, SMS does not involve STIP or the issuer. SMS logs the request and response.
- If processing of the original request is still in progress, SMS logs the duplicate, then discards it. (SMS assumes that the original will be completed; therefore the duplicate is not needed.)

Service Participation Requirements 3

This chapter summarizes the required and optional functionality for Interlink acquirers and issuers. The subsequent chapters of this manual discuss these functions in detail.

General Requirements

Participating acquirers and issuers must meet certain processing and operations requirements. Both issuers and acquirers also have a variety of connection, service, and processing options from which to choose when developing their individual SMS programs.

All SingleConnect participants are responsible for operating a data processing center, or designating one, that has the systems necessary to provide merchant and cardholder support services.

Acquirers and issuers must be able to send and receive the transactions described in this chapter.

Members must have their connections to VisaNet certified by Visa and must successfully complete the Visa certification process. Once certified, they can begin initiating and receiving SMS transactions. Alternatively, members can designate third-party processors to complete the certification process and process SMS transactions on their behalf.

Except where noted, all SMS acquirers and issuers must:

- Use the VisaNet standard V.I.P. ISO message format and observe all rules for its use. To ensure message integrity, acquirers and issuers must keep track of incoming and outgoing messages, recognize and eliminate repeats, and generate reversals for transactions that cannot be completed.
- Use VisaNet Access Point (VAP) Software Release 10.2 or higher.

- Complete technical certification prior to participation in the service. The certification process covers all relevant message types, raw data, and reports. Online certification services are available from your Visa representative.
- Comply with all applicable Visa operating regulations.
- Log all transactions, whether approved or declined, to reconcile to Visa settlement positions.
- Support exception processing, as specified later in this chapter.
- Ensure that Personal Identification Number (PIN) processing requirements meet the standards specified in Chapter 7, Security. PIN is required for Interlink.
- Participate in CVV. Please refer to Card Verification Value (CVV) Service in Chapter 6 for additional information.
- Participate in the VisaNet Settlement Service (VSS)

Acquirer System Requirements

Acquirer systems support merchant magnetic-stripe-reading terminals and, conditionally, PIN pads. Acquirer systems are also the points of interaction between merchants and VisaNet.

Online Transaction Processing

The following transactions must be supported by all Interlink acquirers:

- Purchases
- Balance inquiries
- Reversals
- Adjustments
- Chargebacks
- Representments
- Administrative transactions, which can be submitted using BOAS
- Funds transfers
- Network management transactions
- Response to all transactions

Acquirers must log all financial and nonfinancial transactions, whether the requests are approved or declined, for posting to merchant accounts and reconciling to Visa settlement positions.

Acquirers must be able to forward responses to the points of sale and determine the success of the delivery of the responses. Reversals must be initiated and sent to VisaNet when the responses cannot be delivered successfully to the points of sale.

Required Capabilities for Acquirers

The following capabilities are required for acquirers.

PIN Security

PIN security must be assured from the moment the cardholder enters the PIN until the transaction leaves the acquirer's system. Each Interlink acquirer must be capable of accepting and translating encrypted PINs and performing key management.

See Chapter 7, Security, for more information on transactions that may include a PIN and standards for PIN security.

Exception Processing

Automated exception processing must be supported. For acquirers, this includes the ability to initiate adjustment, representment, and administrative messages, and the ability to receive chargebacks, chargeback reversals, and administrative messages. The Visa BackOffice Adjustment System (BOAS) is an option that can be used to meet this requirement.

Interlink Routing Table Service

Acquirers must participate in the Interlink Routing Service. See Chapter 8, Routing, for more information.

Acquirer Options

Interlink acquirers can use or support the optional transactions, services, and capabilities identified in this section.

Interlink acquirers can use the following optional transactions:

- Purchases with cashback
- Scrip transactions
- Preauthorizations and preauthorization completions
- Merchandise credits
- POS cancellations
- Store-and-forward transactions
- Paper sales drafts (online financial)
- Resubmissions
- Preauthorization reversals
- Reconciliation transactions
- File maintenance transactions

An acquirer that supports preauthorizations must also support preauthorization reversals and store-and-forward transactions.

In addition to the transactions listed above, Interlink acquirers can use or support the services and capabilities listed in Table 3–1.

Table 3–1: Acquirer Options

Options	References
Multicurrency Service	Chapter 5, Multicurrency Support
Dynamic Key Exchange	Chapter 7, Security
Priority Routing Service	Chapter 8, Routing
Visa BackOffice Adjustment System (BOAS)	Chapter 11, Member-to-Visa Connection Options
Choice of one or more VAP options	Chapter 11, Member-to-Visa Connection Options
Choice of report delivery options	Chapter 11, Member-to-Visa Connection Options
Choice of detailed reports	*VisaNet Settlement Service (VSS) User's Guide, Volume 2*
Receipt of raw data files	See the "Files" chapter of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications.*

NOTE: *Participation in CVV is mandatory for issuers and acquirers. Please refer to "Card Verification Value (CVV) Service" in Chapter 6 for additional information.*

Issuer System Requirements

Issuer systems are required to respond to Interlink messages sent from VisaNet. This response is a primary function of issuer systems.

In addition, issuers need to:

- Send chargebacks, administrative messages, and network management messages.
- Receive transaction requests and approve or decline them according to internally defined parameters. Authorizations must occur within a specified issuer response time or VisaNet processes them using stand-in processing (STIP).
- Receive and process advices from STIP.
- Issue cards in accordance with all applicable Visa operating regulations.
- Support PIN processing requirements as defined in Chapter 7, Security.
- Participate in the VisaNet Settlement Service (VSS). See Chapter 9, Settlement and Reconciliation.

Transaction Processing

Participating issuers must support the full set of transactions initiated by Interlink acquirers and VisaNet, including:

Cardholder Transactions

- Purchase
  - Purchase with cashback
  - Scrip
- Preauthorization/Completion
- Merchandise credit
- POS cancellation
- Balance inquiry

Merchant-Authorized Transactions

- Store-and-forward
- Paper sales draft (online financial)
- Resubmissions

System-Generated Transactions

- Reversal
- Preauthorization reversal

Exception Transactions

- Adjustment
- Chargeback
- Representment

Reconciliation Transactions

Online File Maintenance

Administrative Transactions

- Free text message
- Funds transfer

Network Management Transactions

Responses to each of the transactions listed above

Required Capabilities for Issuers

The following capabilities are required for issuers.

PIN Verification

All Interlink issuers must provide PIN verification capability or subscribe to the Visa PIN Verification Service (PVS) if they process transactions with PINs.

Exception Processing

Interlink participants must support exception processing. For issuers, this includes the ability to initiate chargebacks (but *not* chargeback reversals), and accept adjustments (including good faith collections), representments, and administrative messages. Issuers can meet this requirement by using the Visa BackOffice Adjustment System (BOAS).

Interlink issuers must support file maintenance transactions.

Stand-In Processing Parameters

All issuers must supply Visa with parameters to use when the issuer system is unavailable or does not respond to request messages within the required time limit and SMS makes processing decisions on behalf of the issuer.

The time limit may vary by issuer.

Depending on the Visa card product, the parameters can be as simple as specifying that VisaNet should decline all authorizations if the issuer system cannot be reached.

Issuer Options

Additional services and features that can be used by Interlink issuers are listed in Table 3–2.

Table 3–2: Issuer Options (1 of 2)

Options	References
Optional message types: • Account transfer • Reconciliation messages	Chapter 4, Message Types and Flows
Multicurrency Service	Chapter 5, Multicurrency Support
STIP processing: • PIN Verification Service • Exception File Service • Mod-10 Check Digit Verification • Preauthorization Stand-In Service	Chapter 6, Stand-In and Card Verification Value Processing
Card Verification Value (CVV)	Chapter 6, Stand-In and Card Verification Value Processing
Positive Authorization Capacity Management (PACM) Service	Chapter 6, Stand-In and Card Verification Value Processing
Dynamic Key Exchange	Chapter 7, Security
Choice of settlement options	Chapter 9, Settlement and Reconciliation
Visa BackOffice Adjustment System (BOAS)	Chapter 11, Member-to-Visa Connection Options
Choice of one or more VAP options	Chapter 11, Member-to-Visa Connection Options
Choice of report delivery options	Chapter 11, Member-to-Visa Connection Options

Table 3–2: Issuer Options (2 of 2)

Options	References
Choice of detail reports	*VisaNet Settlement Service (VSS) User's Guide, Volume 2*
Receipt of raw data files	*V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*

NOTE: *Participation in CVV is mandatory for issuers and acquirers. Please refer to Card Verification Value (CVV) Service in Chapter 6 for additional information.*

Message Types and Flows 4

This chapter describes the message flows for Interlink transactions. It explains which message types are used and how messages are exchanged. Each flow description includes a diagram showing which messages are passed between the acquirer, issuer, and SMS.

This chapter contains two sections:

- Standard Processing—This section describes the flows for the following transactions processed under standard conditions:
  - Cardholder Transactions
  - Merchant-Authorized Transactions
  - System-Generated Transactions
  - Exception Transactions
  - Reconciliation Transactions
  - File Maintenance Transactions
  - Administrative Transactions
  - Network Management Transactions
- Exception Conditions—This section describes the flows for the following transactions when an endpoint is not available, responds late, or fails to respond:
  - Preauthorizations
  - Financial Transactions
  - Reversals
  - Exception Transactions

Standard Processing

This section describes the following transactions processed under standard conditions.

Cardholder Transactions

The flow diagrams and descriptions in this section illustrate the flows for Interlink transactions initiated by the cardholder.

Purchases

A purchase transaction is a standard purchase request to authorize, post, and settle a transaction involving the sale of goods or services.

Cashback transactions are included in the flows for this category. A purchase with cashback transaction differs from a purchase by an amount in Field 61.1—Other Amounts.

A purchase with cashback transaction is a variation of the purchase transaction that permits the cardholder to get cash in addition to goods or services. This transaction is optional for acquirers and merchants. Merchants that want to support this transaction service establish their own cashback limits.

Keeping the cashback amount separate from the purchase amount allows the issuer to check the desired cashback amount against daily cash withdrawal limits, which may differ from daily purchase limits.

If the desired cashback amount causes the daily cash withdrawal limit to be exceeded, or if the combined purchase and cashback amount exceeds the cardholder's available balance but the purchase amount alone does not, the issuer can decline the transaction by using a response code to indicate that the cashback limit was exceeded, and the merchant can send a new transaction for the purchase amount only.

Scrip transactions are used by merchants that have self-service terminals that dispense scrip. Scrip can be exchanged for goods, services, or cash. Only acquirers in the U.S. region can submit scrip transactions, but all issuers must be prepared to receive scrip transactions. A value of 17 in the Transaction Type subfield of Field 3—Processing Code distinguishes a scrip transaction from a purchase transaction.

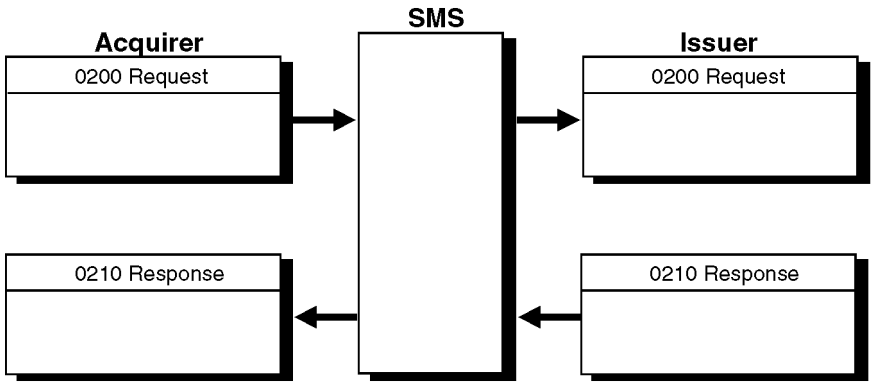
Purchase requests have financial impact on cardholder accounts. They result in the updating of system settlement totals for both the acquirer and issuer.

A standard purchase transaction is composed of two messages:

- An 0200 request generated by the acquirer
- An 0210 response sent by the issuer

Figure 4–1 illustrates the standard flow of a purchase transaction.

Figure 4–1: Purchase Transaction Flow



Preauthorization Request and Completion

Preauthorization transactions are used to authorize transactions in advance of the actual purchase before the final amount of the purchase is known, such as at a gas station. The acquirer is required to initiate two messages to complete the transaction: the *preauthorization request* and the *preauthorization completion*. An approved preauthorization request is valid for two hours.

The acquirer sends the requested preauthorization amount in the 0100 preauthorization requested message. The issuer or STIP processes the transaction, and, if approved, responds with the approved amount. This amount is typically the request amount, but it may be less than the amount in the preauthorization request. Partial approvals are permitted and identified by a value of 10 in Field 39—Response Code. The amount originally requested is contained in Field 61.1—Other Amount, Transaction.

If the preauthorization request is declined, the transaction is terminated at this point. If it is approved, the transaction is temporarily interrupted until the cardholder completes the transaction. An approved preauthorization request holds funds for two hours. After two hours, the issuer approves or declines the transaction at its discretion.

When STIP processes a preauthorization request, it creates an 0120 advice for the issuer. When the issuer recovers this advice, it acknowledges with an 0130 message.

An 0200 preauthorization completion is generated by the acquirer when the transaction is completed. It identifies the specific transaction amount to the issuer and requires an approval response if certain parameters are met. This message enables the issuer to debit the cardholder's account.

An 0210 preauthorization completion response is returned by the issuer or STIP. A preauthorization completion must be approved if the following conditions are met:

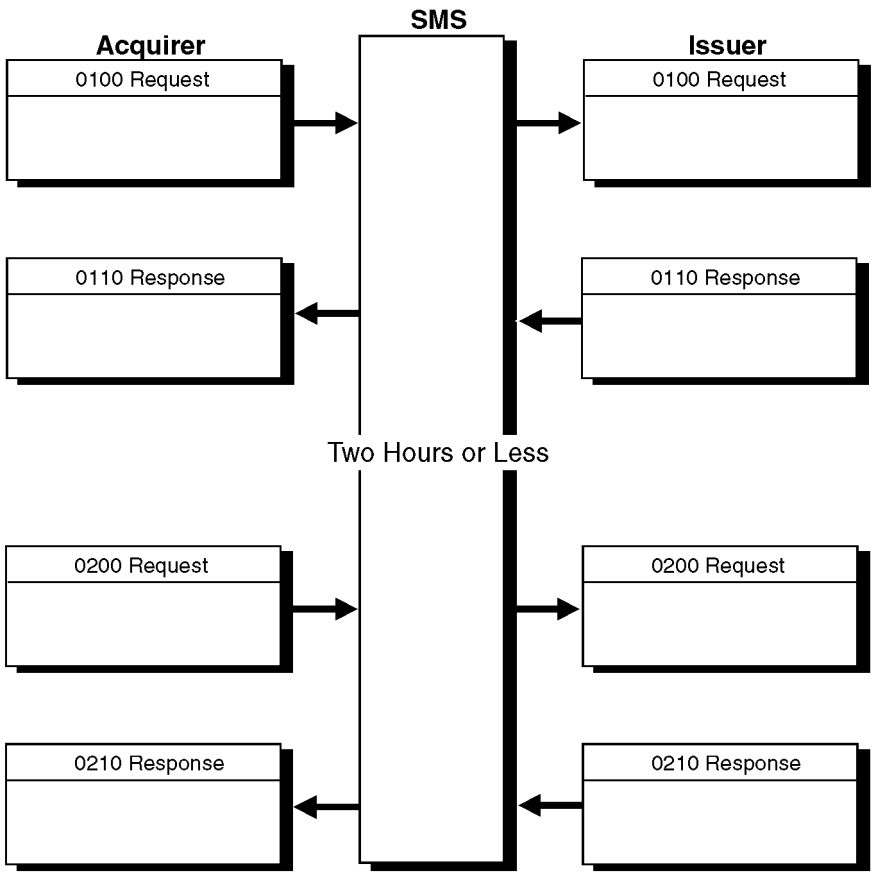
- The preauthorization completion amount does not exceed the preauthorization response amount.
- The preauthorization completion is initiated within two hours of the preauthorization response.
- The acquiring institution, retrieval reference number, and original data elements of the preauthorization completion message match those of an outstanding preauthorization request message.

If these criteria are met and the issuer declines the completion request, SMS rejects the decline response and sends it back to the issuer; simultaneously, STIP approves the preauthorization completion.

An 0210 message containing an approval response results in the updating of settlement totals.

Figure 4–2 illustrates the flow of a preauthorization request (0100) and the subsequent preauthorization completion (0200).

Figure 4–2: Preauthorization Request and Completion Transaction Flow



If the issuer is participating in the Preauthorization Stand-In Service and the preauthorization transaction complies with the conditions stated in this section, STIP approves the transaction and creates an advice for the issuer.

Merchandise Credit

A merchandise credit is a financial transaction that instructs the issuer to credit the cardholder's account for the return of merchandise. The return amount is debited to the acquirer and credited to the issuer.

The return amount must be equal to or less than the amount of the original purchase. Returns for less than the amount of the original purchase occur when the cardholder returns only a portion of the goods originally purchased.

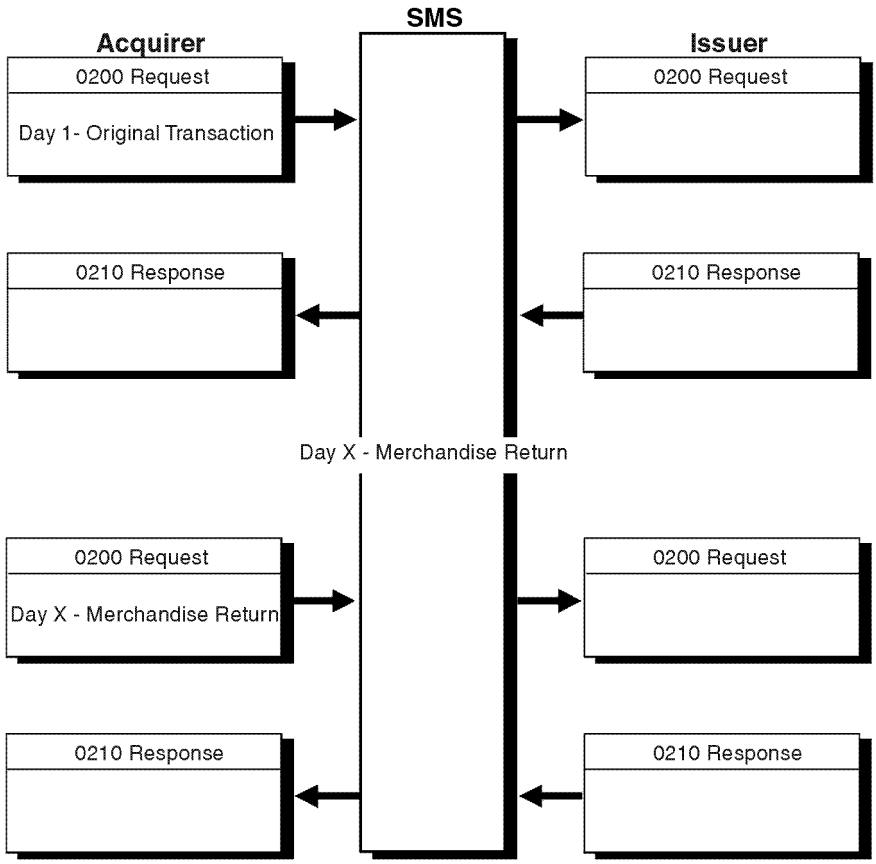
A return is initiated at the point of sale. Use of the same terminal or merchant outlet used for the original purchase is not required.

The card must be read electronically and the PIN entered at the time of the transaction. Returns can occur up to one year after the date of the original purchase. The merchant must enter the local date of the original purchase from the receipt and place it in field 48.

A value of 20 in the first two positions of the processing code (field 3) is used to distinguish returns from other 0200 request messages.

Figure 4–3 illustrates a merchandise credit transaction flow.

Figure 4–3: Merchandise Credit Transaction Flow



POS Cancellation

An Interlink POS cancellation is used when the customer or merchant wants to cancel a previously completed debit request at the point of sale.

A POS cancellation must be processed on the same calendar day as the original transaction, and the dollar amount in the cancellation must equal the dollar amount in the original transaction. Additionally, the cardholder must be present to swipe the card through the magnetic stripe reader and enter the PIN. A POS cancellation is settled only if the transaction being cancelled was settled. The following types of transactions can be cancelled:

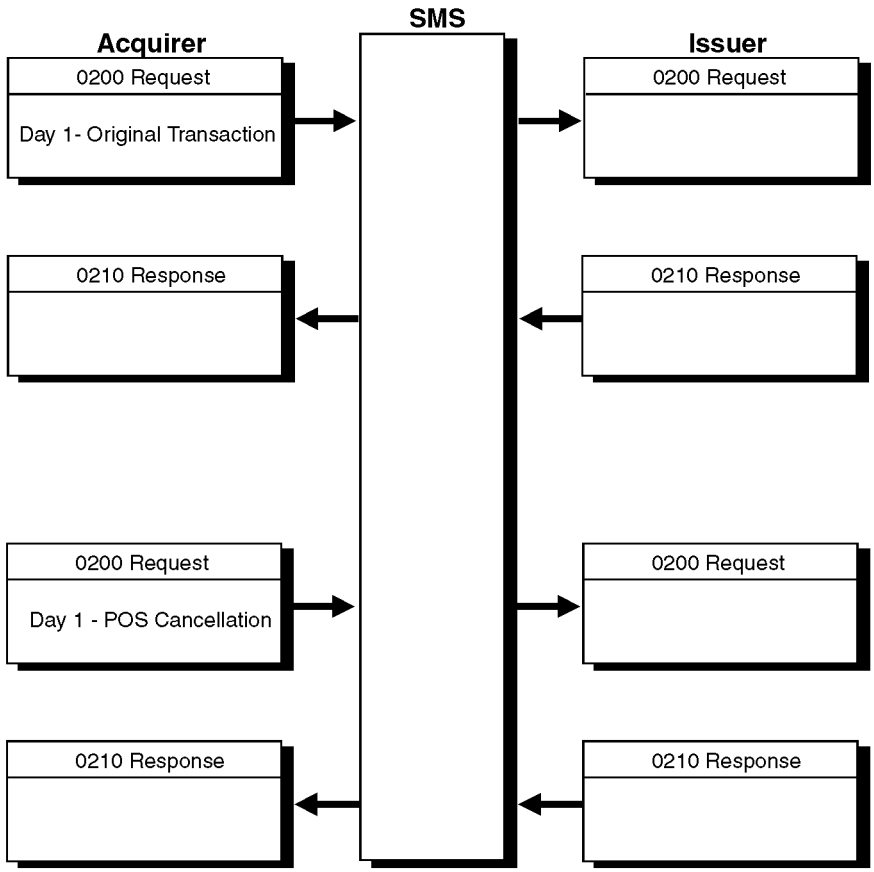
- Purchase transactions
- Purchase with cashback transactions
- Scrip transactions
- Merchandise credits

If the merchant needs to cancel a transaction after the cardholder has left the point of sale, the merchant must ask the acquirer to process an adjustment.

To distinguish the POS cancellation transaction from other 0200 requests, Message Reason Code 2005 is used in Field 63.3—Message Reason Code.

Figure 4–4 illustrates the transaction flow of a POS cancellation.

Figure 4–4: POS Cancellation Transaction Flow



Balance Inquiry

A balance inquiry requests that a savings or checking account balance be displayed at a consumer terminal at a merchant location.

Interlink Multicurrency Service participants use Field 54—Additional Amount for returning balance information in approved balance inquiry responses. SMS always converts the values in the amount fields depending upon members' participation in the Multicurrency Service.

Interlink issuers that do not support multicurrency processing return the available funds in Field 4—Amount, Transaction. Issuers that do not support multicurrency processing can use Field 61.1—Other Amount, Transaction for a second balance.

If the balance is a negative amount, the issuer returns zeros.

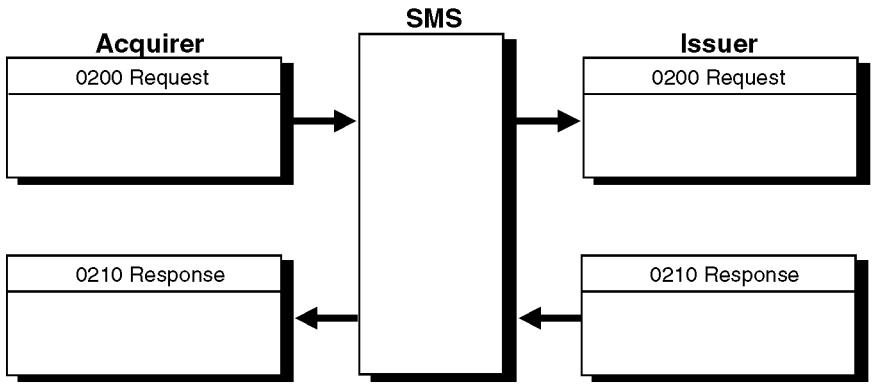
A balance inquiry has no financial interchange value and cannot be reversed.

If STIP returns a decline decision on behalf of the issuer, STIP does not create an advice for the issuer.

To distinguish the balance inquiry from other 0200 requests, a value of 30 is placed in the first two positions of Field 3—Processing Code.

The standard flow of a balance inquiry transaction is illustrated in Figure 4–5. It consists of a balance inquiry request (0200) originated by the acquirer, followed by a balance inquiry response (0210) generated by the issuer.

Figure 4–5: Balance Inquiry Transaction Flow



Merchant-Authorized Transactions

There are three types of Interlink merchant-authorized transactions: store-and-forward, paper sales draft, and resubmission.

Store-and-Forward Original Transaction

An Interlink store-and-forward transaction is used when a merchant cannot complete a purchase or merchandise credit transaction because the acquirer or SMS is unavailable. The uncompleted transaction is stored by the acquirer or merchant pending restoration of the acquirer's system interface to SMS. When communication is restored, the acquirer forwards an 0200 store-and-forward request.

PIN data is required. Store-and-forward transactions can be submitted up to nine calendar days after the date of purchase.

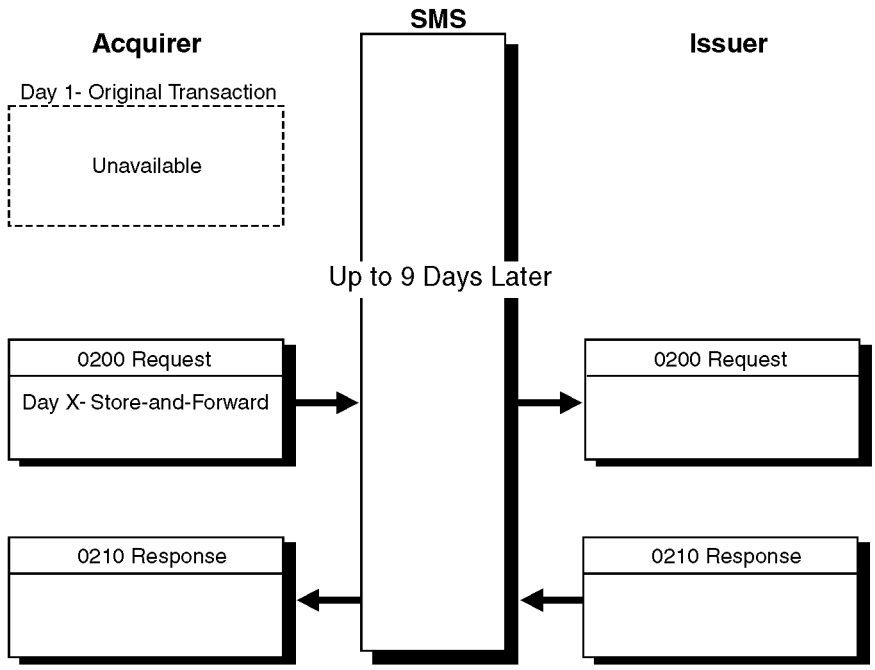
STIP does not approve store-and-forward requests when the issuer is unavailable. SMS returns Response Code 91—Destination Unavailable in Field 39—Response Code.

To distinguish the store-and-forward transaction from other 0200 requests, Message Reason Code 5202—Store-and-Forward Submission must be used in Field 63.3—Message Reason Code.

If the store-and-forward transaction is declined for nonsufficient funds or because daily limits or cashback limits are exceeded, the acquirer can resubmit it as a resubmission transaction with Reason Code 5204—Store-and-Forward Resubmission in Field 63.3—Message Reason Code. The "Resubmission" section of this chapter describes this flow.

Figure 4–6 illustrates the store-and-forward transaction flow.

Figure 4–6: Store-and-Forward Transaction Flow



Paper Sales Draft (Original Submission)

Interlink paper sales drafts are used when a merchant cannot complete a transaction because of problems with the terminal. When allowed by the acquirer, merchants can use paper sales drafts and later submit the sales drafts to their acquirers.

Acquirers then submit electronic paper sales draft transactions. Acquirers have the option of entering the paper sales drafts using the BackOffice Adjustment System (BOAS).

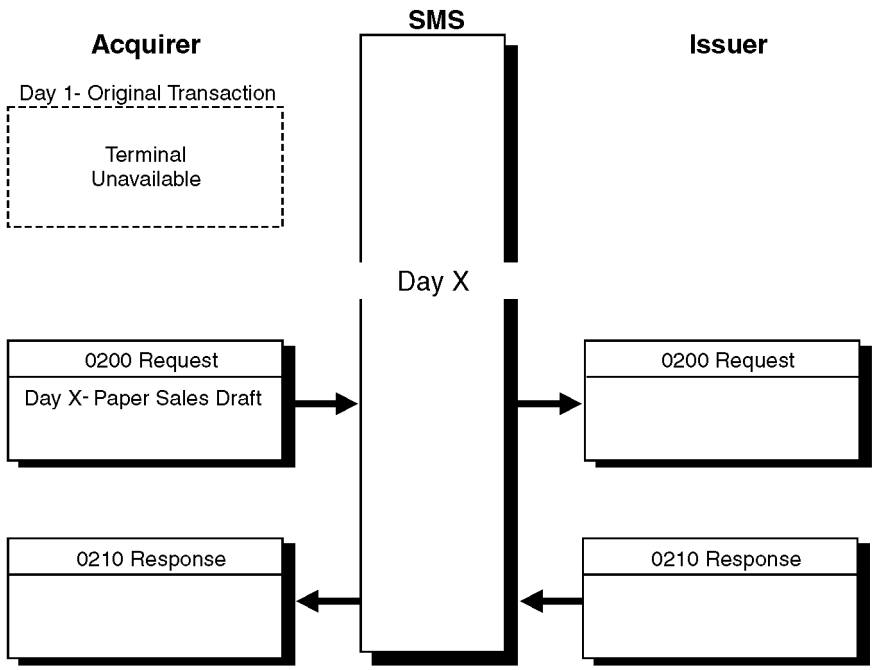
STIP does not approve paper sales drafts when the issuer is down. SMS returns Response Code 91—Destination Unavailable in Field 39—Response Code.

To distinguish the paper sales draft from other 0200 requests, the acquirer must use Message Reason Code 5201—Paper Sales Draft Submission in Field 63.3—Message Reason Code.

If the paper sales draft transaction is declined for insufficient funds or because daily purchase or cashback limits are exceeded, the acquirer can resubmit it as a resubmission transaction with Message Reason Code 5205—Paper Sales Draft Resubmission in Field 63.3—Message Reason Code. The "Resubmission" subsection of this chapter describes this flow.

Figure 4–7 illustrates the transaction flow of a paper sales draft.

Figure 4–7: Paper Sales Draft Transaction Flow



Resubmission

An Interlink resubmission is used when a merchant cannot complete a transaction because the original request was declined due to insufficient funds or because daily purchase limits or cashback limits are exceeded.

Field 39 response codes that qualify for resubmission include:

51 = Not sufficient funds

61 = Exceeds approval amount limit

65 = Exceeds withdrawal frequency limit

82 = Cashback limit exceeded (valid only for resubmission of store-and-forward and paper sales draft transactions)

In the standard processing flow, the acquirer generates an 0200 resubmission on Day Two when a transaction has been declined by the issuer on Day One. The earlier information from the declined transaction is provided in Field 90—Original Data Elements.

If the transaction is again declined for nonsufficient funds (NSF), because daily purchase or cashback limits are exceeded, or because the issuer is unavailable, the acquirer can continue to resubmit the transaction once each day for up to nine calendar days following the original request.

STIP does not approve resubmissions when the issuer is unavailable. SMS returns Response Code 91—Destination Unavailable in Field 39—Response Code.

If acquirers receive Response Code 91—Destination Unavailable in Field 39—Response Code, they can retry the transaction on the same day.

The acquirer has the option of entering resubmissions of paper sales drafts using BOAS; however, other types of resubmissions cannot be submitted using BOAS.

To distinguish the type of transaction being resubmitted, the following message reason codes are used in Field 63.3—Message Reason Code:

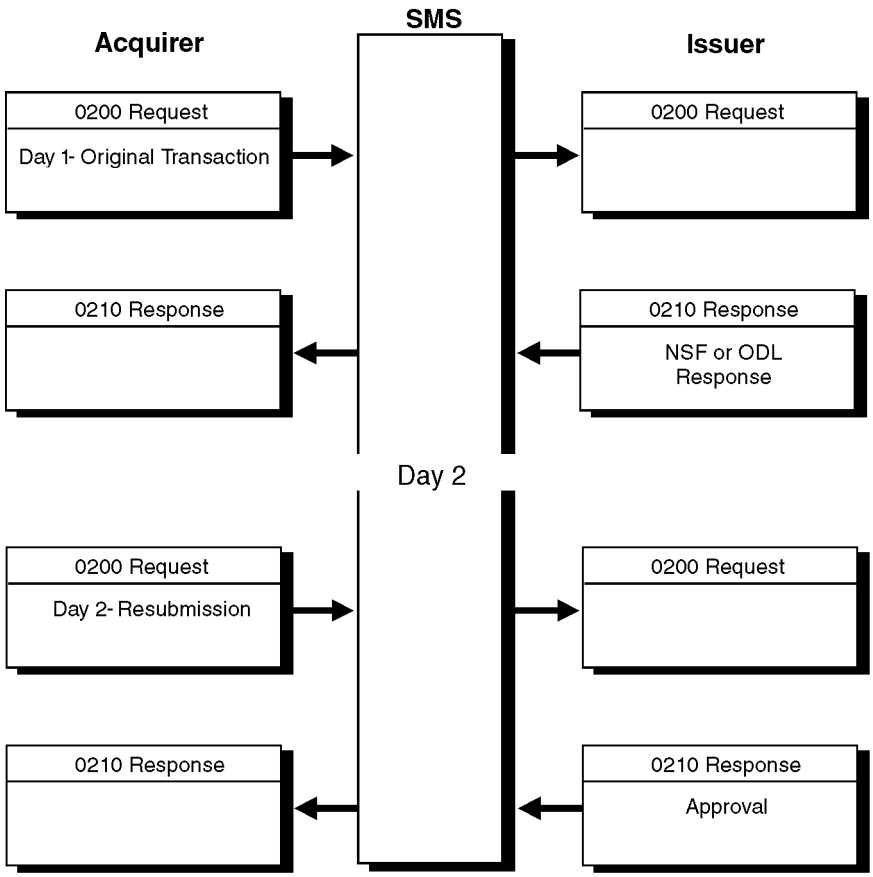
5203 = Online resubmission (cannot be resubmitted using BOAS)

5204 = Store-and-forward resubmission (cannot be resubmitted using BOAS)

5205 = Paper sales draft resubmission (can be resubmitted using BOAS)

Figure 4–8 illustrates the transaction flow for a resubmission.

Figure 4–8: Resubmission Transaction Flow



System-Generated Transactions

For Interlink, system-generated transactions consist of reversals only.

Reversals

A reversal cancels an authorization or voids a financial transaction. Either SMS or the acquirer's system can generate a reversal. Only full reversals are supported by SMS. Reversals can have settlement impact. An acquirer-generated reversal of a declined transaction has no settlement impact.

An acquirer uses 0420 reversal advices for the following reasons:

- A previously approved preauthorization (0100) or financial transaction (0200) is cancelled at the point of service because the cardholder does not complete the transaction or the merchant makes an error that requires voiding.

  Message reason code 2501 applies to such advices.

- The acquirer does not receive a response to an 0100 or 0200 request and does not know if the request was approved or declined (message reason code 2502).

- An approval response arrives after the acquirer or the point-of-service device has timed out (message reason code 2502).

- The acquirer cannot send an approved response to the point of service (message reason code 2503).

- The acquirer receives approval of an 0100 or 0200 request and sends it to the point of service but does not receive a completion message from the point of service (message reason code 2503).

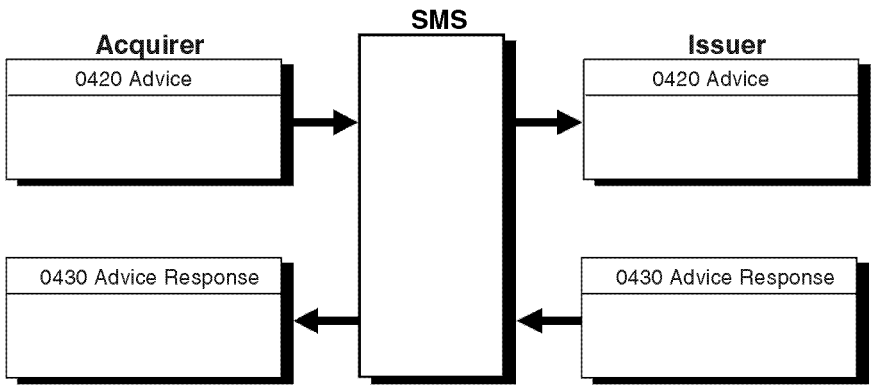
SMS uses 0420 advices when it cannot return 0210 approvals to an acquirer or cannot forward a reversal request to an issuer.

A reversal cannot be declined or reversed. On receipt of a reversal, the issuer should release its hold on funds or reverse the posted transaction from the cardholder's account and from its settlement totals. Reversals are generated to prevent errors in settlement and reconciliation and to enable an issuer to adjust any service charges to the cardholder's account.

Under normal conditions, the acquirer submits an 0420 reversal advice to the issuer, and the issuer returns an 0430 response. Some acquirers, using an earlier implementation of V.I.P. ISO, can submit 0400 requests, and issuers must be able to receive them. If the acquirer sends an 0400 request to the issuer, the issuer acknowledges with an 0410 response. An 0410 response must be used to respond to an 0400 reversal. Visa recommends that acquirers use 0420 advices.

Figure 4–9 illustrates a standard reversal transaction flow.

Figure 4–9: Reversal Transaction Flow



Exception Transactions

Interlink supports the following exception transactions:

- Adjustments
- Good Faith Collection
- Chargebacks
- Representments

Adjustments

A back office adjustment is used by acquirers when a processing error has been identified, typically through the reconciliation process. For example, during reconciliation a duplication of a transaction is discovered. Adjustment advices are entered by the acquirer's operations staff, not at the point of sale.

Interlink acquirers must submit adjustments within 45 calendar days from the date of the original transaction.

There are two types of adjustment transactions:

- Debit adjustments (processing code 02*xxxx*)—These transactions are used when the cardholder's account was charged less than the actual transaction amount.
- Credit adjustments (processing code 22*xxxx*)—These transactions are used when one of the following conditions applies:
  - A cardholder's account was charged more than the actual transaction amount.
  - The cardholder's account was charged for an invalid transaction.

Acquirers have the option of entering adjustments using the BackOffice Adjustment System (BOAS). Issuers can receive adjustments through BOAS.

Adjustments may be issued on all types of purchase transactions, including cashback, scrip transactions, and preauthorization completions. Only one adjustment can be issued for a transaction.

To distinguish the adjustment from other transactions, the message reason code in field 63.3 must be 2004.

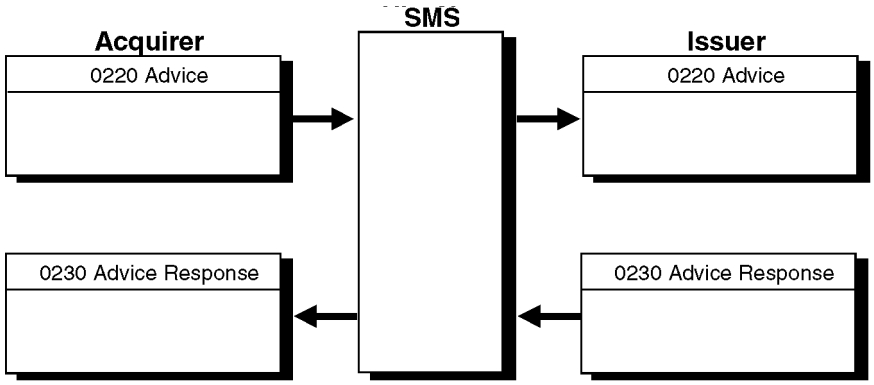
An 0220 adjustment advice is sent by the acquirer. An 0230 advice response is returned by the issuer or STIP to acknowledge to the acquirer that the adjustment advice was successfully received. An issuer cannot decline an adjustment, although it can charge it back if chargeback/return rights exist. The approval by the issuer indicates the adjustment has been received; it does not indicate that the issuer is in agreement with the adjustment.

The acquirer cannot reverse an adjustment. Issuers can return invalid debit adjustments or credit adjustments through chargeback transactions, and acquirers can re-present adjustments.

If an adjustment transaction times out (that is, an 0230 advice response is not received), the acquirer must resend the adjustment unchanged with the same tracing elements.

Figure 4–10 illustrates a standard (back office) adjustment transaction flow.

Figure 4–10: Adjustment Transaction Flow



Good Faith Collection

A good faith collection is an adjustment transaction that cannot be processed according to standard Interlink processing procedures, typically because the time frame has expired. Ordinarily, Interlink acquirers must submit adjustments within 45 calendar days from the date of the original transaction, but this edit is not enforced for good faith collection transactions.

Good faith collections are allowed only after both parties agree to the collection.

There are two types of good faith collection transactions:

- Good faith debit adjustments—These transactions use processing code 02*xxxx*.
- Good faith credit adjustments—These transactions use processing code 22*xxxx*.

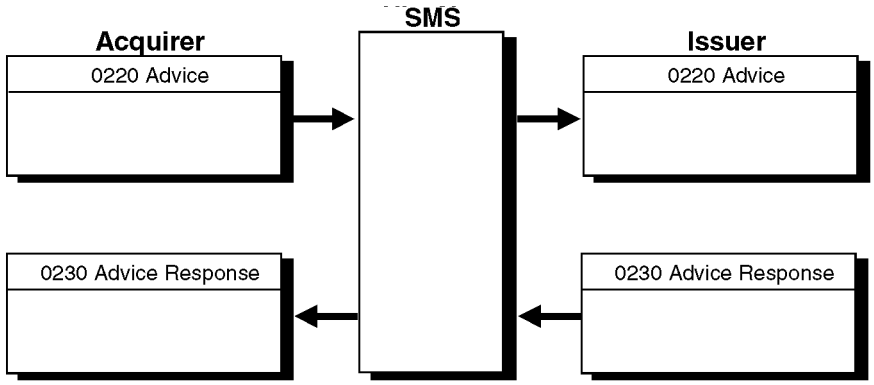
Acquirers have the option of entering good faith collections using BOAS. Issuers can elect to receive good faith collections through BOAS.

The message content specifications for a good faith collection are the same as those for an adjustment transaction, except that Field 125—Supporting Information must contain a value of "GFC" (good faith collection) in the first three positions of the Unformatted Text subfield.

Field 63.3—Message Reason Code must contain 2004.

The good faith collection transaction flow is illustrated in Figure 4–11.

Figure 4–11: Good Faith Collection Transaction Flow



Chargebacks

An issuer uses a chargeback to return a previously accepted financial transaction to an acquirer. Issuers have the right to charge back to the acquirer posted transactions that are disputed by the cardholder or identified as invalid by the issuer. Chargebacks must adhere to applicable Visa operating regulations.

Chargebacks must be submitted within a set number of calendar days from the origination date of the transaction being charged back. Interlink chargebacks, which are governed by the *Interlink Program Operating Regulations (Visa International Operating Regulations, Volume IV)*, must be submitted within 100 calendar days of the transaction being charged back, with two exceptions:

- If a chargeback transaction contains a message reason code of 2480 (invalid/unpostable adjustment), the chargeback must be submitted within 10 days of the adjustment.
- For a merchandise credit, the issuer can exercise the chargeback right only after 10 calendar days from the transaction date of the merchandise credit.

The chargeback amount should be for the original amount or less, and should not include optional issuer fees. Partial chargebacks are allowed when the cleared amount exceeds the authorized amount.

The issuer has the option of entering chargebacks using the BackOffice Adjustment System (BOAS). The acquirer can elect to receive chargebacks through BOAS.

The chargeback flows from the issuer to the acquirer—the opposite direction from other financial transactions. The response by the acquirer acknowledges that the chargeback was successfully received and processed. The response does not signify that the acquirer is in agreement with the request.

Acquirers use representments to return invalid chargebacks.

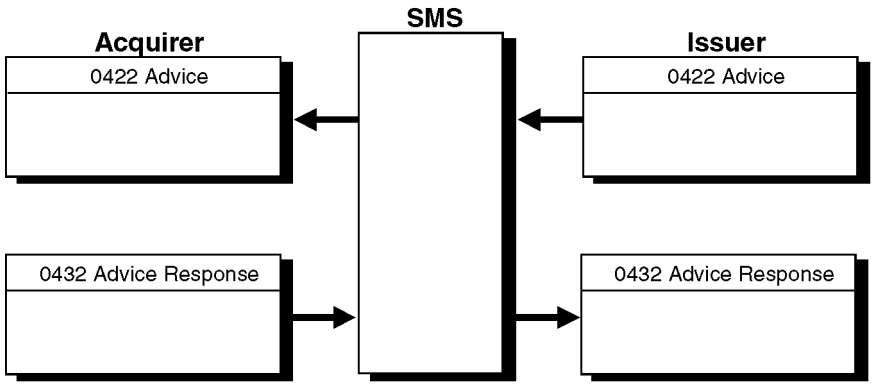
If the chargeback times out at the issuer, the issuer should resend the chargeback transaction unchanged.

A chargeback can be distinguished from other messages of the same message type by the value of 17 in Field 25—Point of Service Condition Code. Reasons for chargebacks are identified in Field 63.3—Message Reason Code.

Only one chargeback transaction can be processed for a cardholder transaction.

Figure 4–12 illustrates a chargeback transaction flow.

Figure 4–12: Chargeback Transaction Flow



Representments

An acquirer uses a representment to resubmit a transaction that was charged back by an issuer. An acquirer can resubmit to the issuer any item that was previously charged back by the issuer. Interlink representments are governed by the *Interlink Program Operating Regulations (Visa International Operating Regulations, Volume IV),* and acquirers must submit them within 15 calendar days of the chargeback transactions.

The acquirer has the option of entering representments using the BackOffice Adjustment System (BOAS). The issuer can elect to receive representments through BOAS.

A representment cannot be reversed or declined.

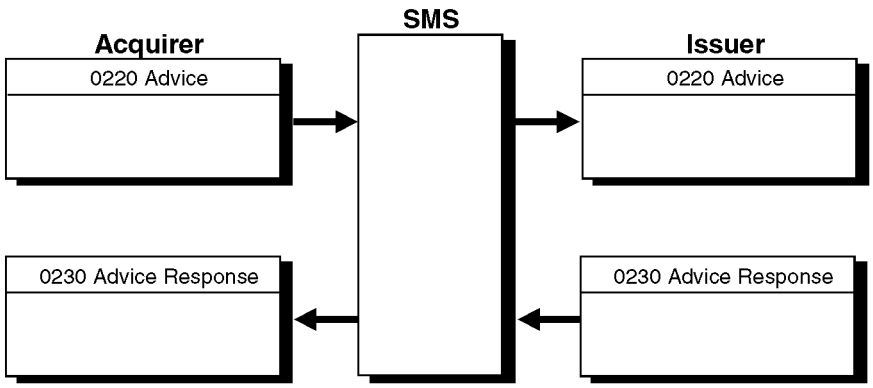
An approval response from the issuer or STIP acknowledges that the request was received, not that the issuer agrees with the request.

If the representment times out at the acquirer, the acquirer should resend the representment unchanged.

A representment can be distinguished from other messages of the same message type by a code of 13 in Field 25—Point of Service Condition Code. Reasons for representments are identified in Field 63.3—Message Reason Code. Interlink has separate codes for chargebacks and representments.

Figure 4–13 illustrates a representment transaction flow.

Figure 4–13: Representment Transaction Flow



Reconciliation Transactions

Reconciliation messages are used to provide issuers and acquirers with current gross interchange totals.

Issuers and acquirers can request and receive cumulative reconciliation advices from Visa at any time. In addition, SMS can send advices automatically at the end of a settlement day (see the "Automatic Reconciliation Advices" subsection later in this chapter).

Throughout the day, SMS accumulates counts and amounts of transactions that affect a participant's financial positions. Totals are available for the current and previous days.

The following subsections describe processing for requested advices and automatic advices.

Requested Reconciliation Advices

Members can initiate an online totals message at any time requesting that SMS create issuer and acquirer reconciliation totals. An 0800 network management message is used to request totals, with the value in Field 70—Network Management Information Code indicating either of the following:

- 270—Cumulative totals of the current day, from start of processing to the time of the request for the reconciliation advice
- 280—Previous day's totals (useful when totals are not available at end-of-day cutoff)

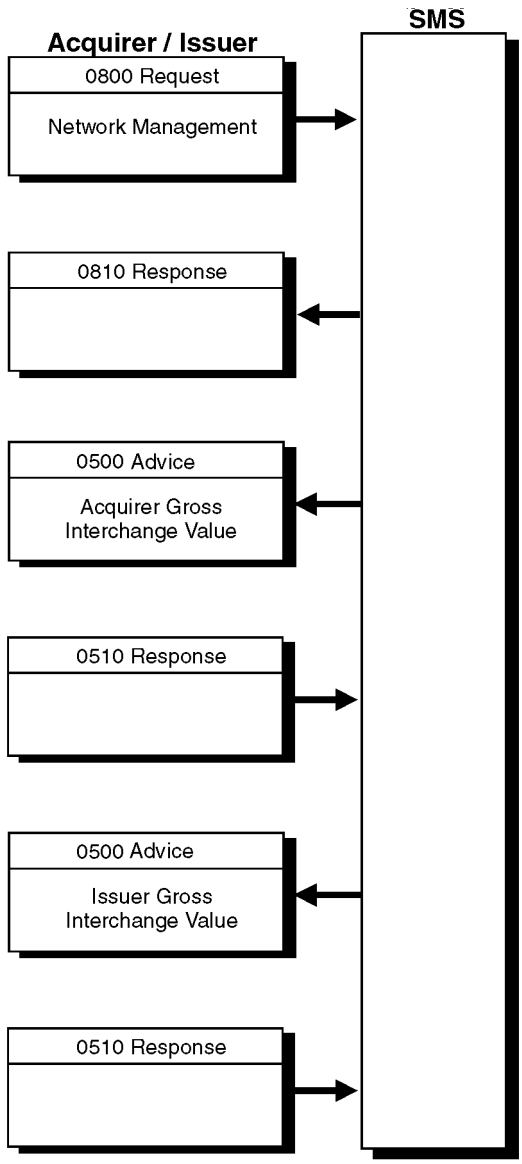
SMS responds to the 0800 message with an 0810 message and then provides the acquirer or issuer with two 0500 messages:

- One contains the Acquirer Gross Interchange Value (acquirer totals plus acquirer STIP totals, if applicable)
- The other contains the Issuer Gross Interchange Value (issuer totals plus acquirer STIP totals, if applicable)

The member responds to each of these messages with 0510 responses.

Figure 4–14 illustrates the reconciliation transaction process.

Figure 4–14: Reconciliation Transaction Flow



Automatic Reconciliation Advices

SMS uses 0520 advice messages to send end-of-day reconciliation totals to acquirers and issuers. The reconciliation totals are provided for the Settlement ID contained in Field 99—Settlement Institution ID Code.

These advices are created automatically and contain the counts and amounts accumulated by SMS for approved, settled transactions.

Each 0520 advice contains one of the following:

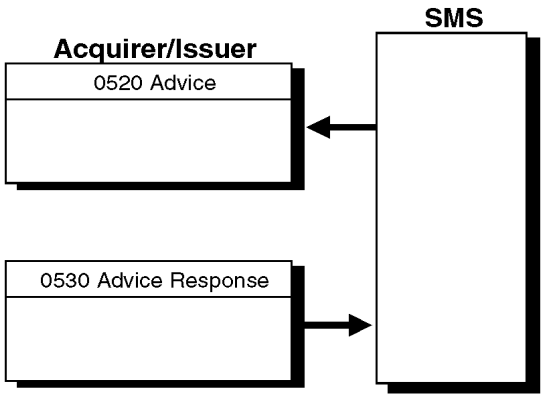
- Acquirer Totals—The value of approved requests and advices sent from the acquirer, as well as chargebacks, chargeback reversals, and fee collection/funds disbursements received from SMS issuers.
- Issuer Totals—The value of chargebacks, chargeback reversals, and fee collection/funds disbursements, as well as approved requests and advices originated by an SMS acquirer.
- Acquirer Stand-In Totals—The value of SMS-generated reversal advices stored by SMS for the acquirer to recover
- Issuer Stand-In Totals—The value of STIP and SMS-generated advices stored by SMS for the issuer to recover

The member acknowledges with an 0530 response message.

Receipt of 0520 advices is optional; they can be sent at the end of day or not at all. The option to receive 0520 messages is set up in SMS when a participant first certifies. Participants can change this option by contacting their Visa representatives. Members must sign on to advice recovery mode to receive advices.

Figure 4–15 illustrates an automatic reconciliation transaction flow with an 0520 optional advice message.

Figure 4–15: Reconciliation Transaction Flow (With an 0520 Optional Advice)



File Maintenance Transactions

This section covers online file maintenance transactions.

For information on batch file updates, refer to the *V.I.P. System SingleConnect SMS Interlink Technical Specifications*.

Online File Maintenance

File-related messages are used by issuers to update or review the cardholder records in the Exception and PIN Verification Files.

An issuer uses an 0302 request to:

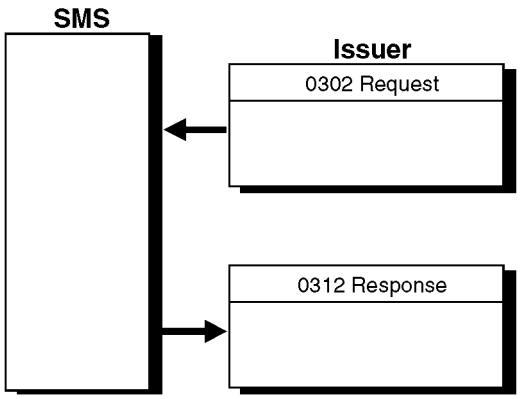
- Update cardholder records.
- Inquire about a specific cardholder record.

An 0302 request is used to query or update both the Exception and PIN Verification Files. SMS does not create advices for undeliverable 0302 requests.

The issuer sends an 0302 request to SMS, and SMS responds with an 0312 response. Because SMS does not create any file-related advices, the issuer must resend the request later if it does not receive an 0312 response from SMS.

Figure 4–16 illustrates a file maintenance transaction flow.

Figure 4–16: Online File Maintenance Transaction Flow



Administrative Transactions

There are two types of administrative transactions:

- Free text message
- Funds transfer message

The following subsections describe each of these transactions.

Free Text Message

A free text message is an administrative message used to convey information from a sender to a receiver. Acquirers and issuers can communicate with each other and get general information from each other by sending free text messages. The originating center submits an 0600 request to the destination center and receives an 0610 response from the destination center. This response contains a no-text reply. If the text from the originating center's 0600 request requires a text reply, the destination center must initiate an 0600 text message with the reply.

SMS accepts free text messages for the destination member when the destination is unavailable. The system stores an 0620 advice in the advice queue to be recovered by the destination member. The 0620 advice requires an 0630 response.

The BackOffice Adjustment System (BOAS) supports these messages.

Figure 4–17 and Figure 4–18 illustrate free text message transaction flows for acquirer to issuer and issuer to acquirer.

Figure 4–17: Free Text Message Transaction Flow (Acquirer to Issuer)

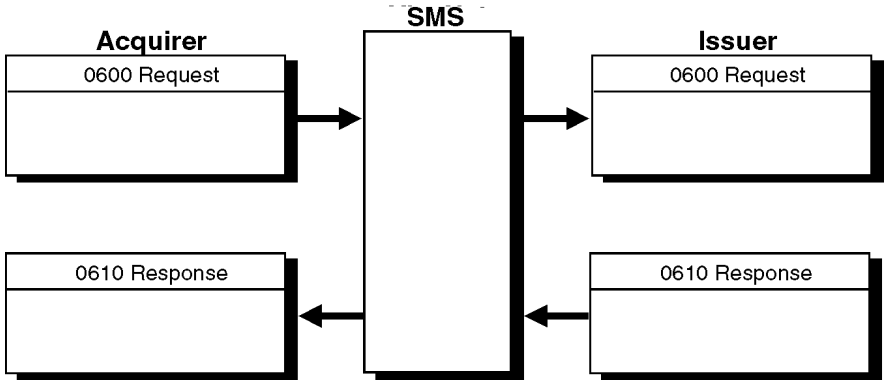
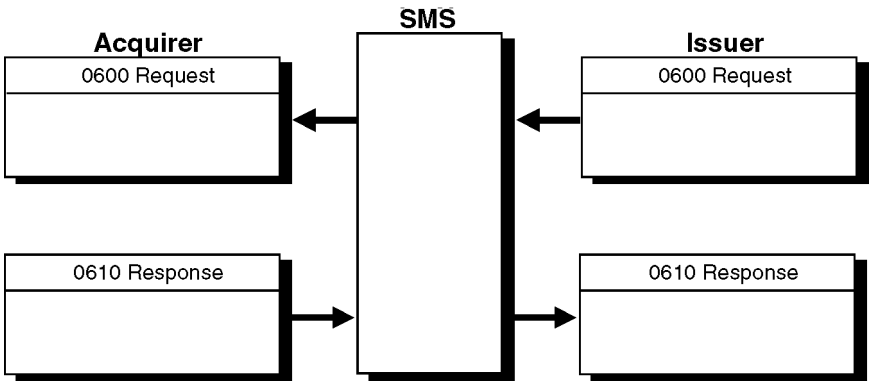


Figure 4–18: Free Text Message Transaction Flow (Issuer to Acquirer)

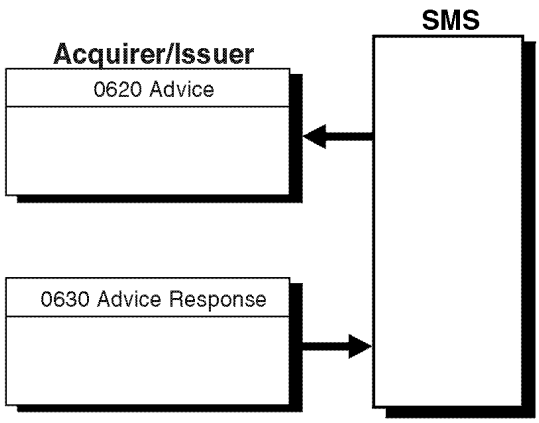


Funds Transfer Message

SMS uses 0620 advices to send the day's final funds transfer totals after completion of settlement and reconciliation. Field 48—Funds Transfer Totals (usage 6) contains the settlement totals for the day, including subfields with acquirer, issuer, and net funds transfer totals. The funds transfer message advises the amount to be transferred to or from the Settlement Account for the Settlement ID contained in Field 99—Settlement Institution ID Code. An 0630 advice response is required for each 0620 request. Members must sign on to advice recovery mode to receive funds transfer messages.

Figure 4–19 illustrates a funds transfer message transaction flow.

Figure 4–19: Funds Transfer Message Transaction Flow



Network Management Transactions

All network management transactions are supported for Interlink.

An acquirer or issuer uses 0800 network management messages to:

- Sign on to and sign off from the system network.
- Perform an echo test of the communication line. (SMS also uses 0800 messages to perform echo tests.)
- Start and stop recovery of advices.
- Perform online dynamic key exchange.
- Solicit the gross interchange totals accumulated for a settlement entity (shown in the reconciliation message flows earlier in this chapter).

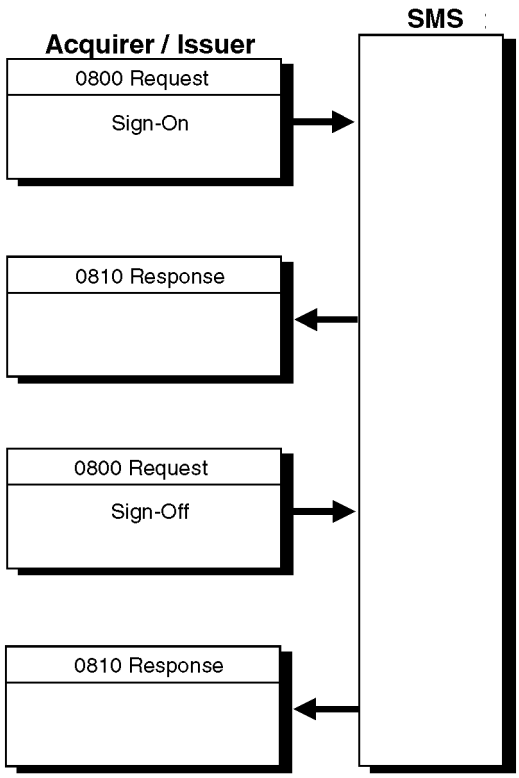
Sign-On and Sign-Off Messages

Each network endpoint must sign on to identify itself to the network. An endpoint can sign on as both an acquirer and issuer. An endpoint signs on to notify SMS that it is ready to send and receive messages. Conversely, an endpoint signs off to notify SMS that it is not available. Endpoints use the network management requests and responses (0800 and 0810) with a value of 071 (to sign on) or 072 (to sign off) in Field 70—Network Management Information Code.

Issuers and acquirers typically sign off for planned maintenance activity or to attend to software or hardware malfunctions.

Figure 4–20 illustrates a sign-on and sign-off message transaction flow.

Figure 4–20: Sign-On and Sign-Off Message Transaction Flow

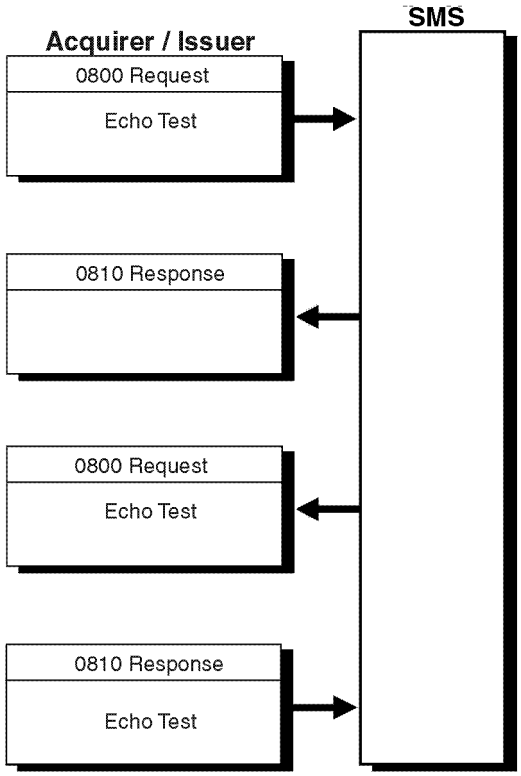


Echo Test Messages

Echo tests confirm the availability of the communications link between the acquirer or issuer and SMS. Network management requests and responses (Message Types 0800 and 0810, respectively) are sent by issuers, acquirers, or SMS to perform echo tests. The value in Field 70—Network Management Information Code in an echo test request is set to 301.

Figure 4–21 illustrates an echo test message transaction flow.

Figure 4–21: Echo Test Message Transaction Flow



Recovery Sign-On and Sign-Off Messages

These messages are used by issuers or acquirers to request and receive advices for transactions that were processed by STIP because there was no response, a late response, or the issuer or acquirer was not available to respond. Acquirers and issuers must sign on to advice recovery mode to receive 0520 automatic reconciliation advices. Network management requests and responses (Message Types 0800 and 0810, respectively) are used with a value of 078 (for sign-on recovery) or 079 (for sign-off recovery) in Field 70—Network Management Information Code.

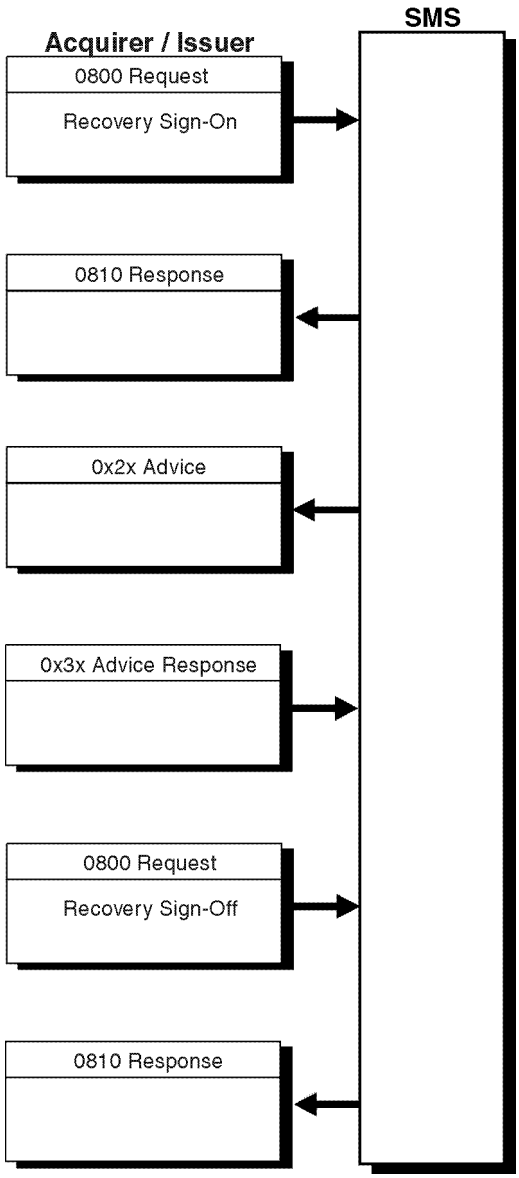
Acquirer and Issuer Recovery

After an issuer or acquirer signs on to advice recovery mode, SMS sends all of the advices (0*x*2*x* messages) that STIP authorized while the issuer or acquirer was unavailable. The issuer or acquirer has the option of remaining signed on to recovery or signing off recovery.

Typically, an issuer or acquirer remains signed on to advice recovery mode so that any transactions processed by STIP are obtained by its system as soon as possible.

Figure 4–22 illustrates a recovery sign-on and sign-off message transaction flow.

Figure 4–22: Recovery Sign-On and Sign-Off Message Transaction Flow



Dynamic Key Exchange

The Dynamic Key Exchange (DKE) Service is an optional Visa service for SingleConnect members that periodically want to change acquirer and issuer Data Encryption Set (DES) encryption working keys through the exchange of online 0800/0810 messages.

The following fields in the 0800 request are used in the key exchange service:

Field 7—Transmission Date and Time

Field 11—System Trace Audit Number

Field 33—Forwarding Institution Identification Code

Field 39—Response Code

Field 48—Additional Data, Private, usage 14 (Dynamic Key Exchange Working Key Check Value)

Field 53—Security Related Control Information

Field 63—SMS Private Use Field (Network ID Code)

Field 70—Network Management Information Code

Field 96—Message Security Code

Members use 0800 requests to request and deliver new working keys for PIN encryption; 0810 responses are used to acknowledge their receipt. The trace number (in field 11) is assigned by the 0800 message originator, which can be a participating acquirer or issuer, or SMS. It must be returned unchanged in the 0810 response. If a new request has to be re-sent, its trace number comes from the original request. The message originator must indicate which key is to be changed in Field 53—Security Related Control Information.

Acquirers can begin using the new key after the 0810 response is sent to SMS. For acquirers supporting a single working key, SMS has the option of processing messages with the new or old key for five minutes. After five minutes, all acquirer-generated messages must have PINs encrypted with the new working key.

For issuers, SMS begins using the new key upon receiving the 0810 response (in which the value in Field 39—Response Code is 00). For issuers supporting a single working key, it immediately updates its copy of the key upon receiving the 0800 response from SMS. SMS continues sending messages with the old key until it receives the 0810 response. Therefore, single-key issuers must keep a copy of the old key until SMS begins using the new one.

For members automatically receiving new working keys on a daily basis, SMS always sets the PIN algorithm identifier (Field 53—Security Related Control Information, positions 3 and 4) to the alternate key. If SMS encounters PIN block errors during standard message processing, SMS returns Response

Code 81—Cryptographic Error Found in PIN in the 0800 request and initiates an automatic acquirer key change. If the issuer encounters a PIN block error during verification, it returns Response Code 81 in the 0810 response. SMS then initiates an automatic working issuer key change.

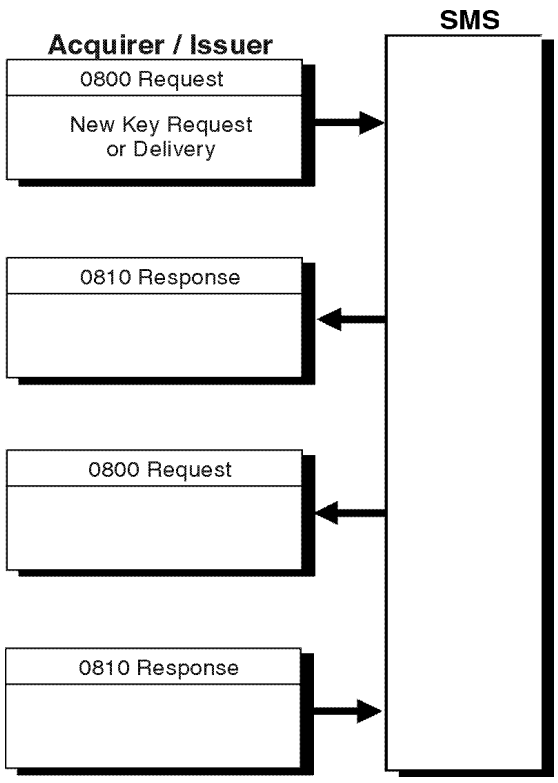
SMS has a 10-second time-out for all dynamic key exchange messages containing new working keys. If the member does not respond within 10 seconds, SMS makes a second delivery attempt. If the member still fails to respond, SMS cancels the key exchange attempt.

An 0800 online message includes a 4-digit key check value (in field 48, usage 14) to verify receipt of the new cryptographic key. Members should compare the four check digits returned from their security module with the check value in the message.

If the key check value (KCV) does not match or if the member encounters a security module error while attempting to translate the new key for storage, the member should return a response code of 06 in field 39. This response indicates that the new cryptographic key has not been received properly.

Figure 4–23 illustrates a dynamic key exchange message transaction flow.

Figure 4–23: Dynamic Key Exchange Message Transaction Flow



Exception Conditions

This section describes the transaction processing that occurs when an endpoint:

- Is not available.
- Fails to respond.
- Responds late.

IMPORTANT

Members must sign on to advice recovery mode to receive advices.

Exception conditions can apply to the following transactions:

- Preauthorizations
  - Preauthorization—Issuer Unavailable
  - Preauthorization—Issuer Unavailable for Preauthorization Completion
  - Preauthorization—Issuer Participates in Preauthorization Stand-In Service
  - Preauthorization—Acquirer Unavailable After Preauthorization Request—Request Declined
  - Preauthorization—Acquirer Unavailable After Preauthorization Request—Request Approved
  - Preauthorization—Acquirer Unavailable After Preauthorization Completion Request; Completion Request Declined
  - Preauthorization—Acquirer Unavailable After Preauthorization Completion Request; Completion Request Approved
  - Preauthorization—Acquirer Receives Reversal From Merchant After Preauthorization
  - Acquirer or SMS Unavailable After Completion of Preauthorization Request
- Financial Transactions
  - Issuer Unavailable
  - Issuer Unavailable—Account Listed on Exception File
  - Issuer Fails to Respond
  - Issuer Responds Late
  - Approval Response Cannot Be Delivered to the Acquirer

  - Decline Response Cannot Be Delivered to the Acquirer

- Reversals
  - Reversal—Advice Response Cannot Be Delivered to the Acquirer
  - Reversal—Issuer Unavailable
  - Reversal—Unsolicited
- Exception Transactions
  - Adjustment or Representment—Issuer Unavailable
  - Adjustment or Representment—Acquirer Unavailable After Advice
  - Chargeback—Acquirer Unavailable
  - Chargeback—Issuer Unavailable After Chargeback

The following subsections describe processing procedures for each of these conditions.

Preauthorizations

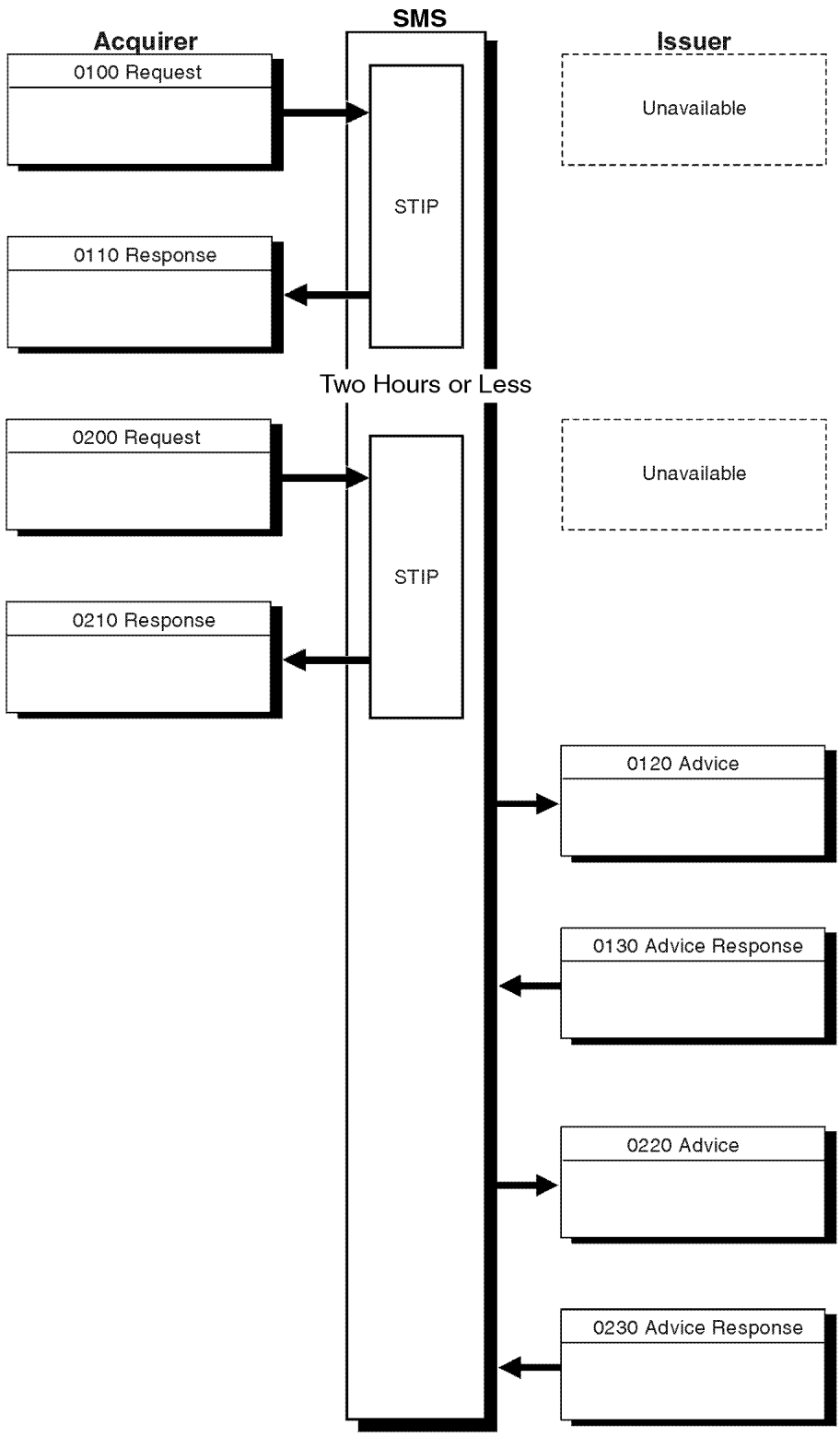
This section describes exception condition processing for preauthorizations.

Preauthorization—Issuer Unavailable

In this flow, STIP handles the transaction because the issuer is unavailable for the entire preauthorization transaction. STIP processes the 0100 and 0200 request messages according to established issuer-unavailable parameters. It returns 0110 and 0210 response messages to the acquirer. The 0110 and 0210 messages are stored in the advice file for recovery by the issuer.

Figure 4–24 illustrates the transaction flow for a preauthorization transaction in which the issuer is unavailable.

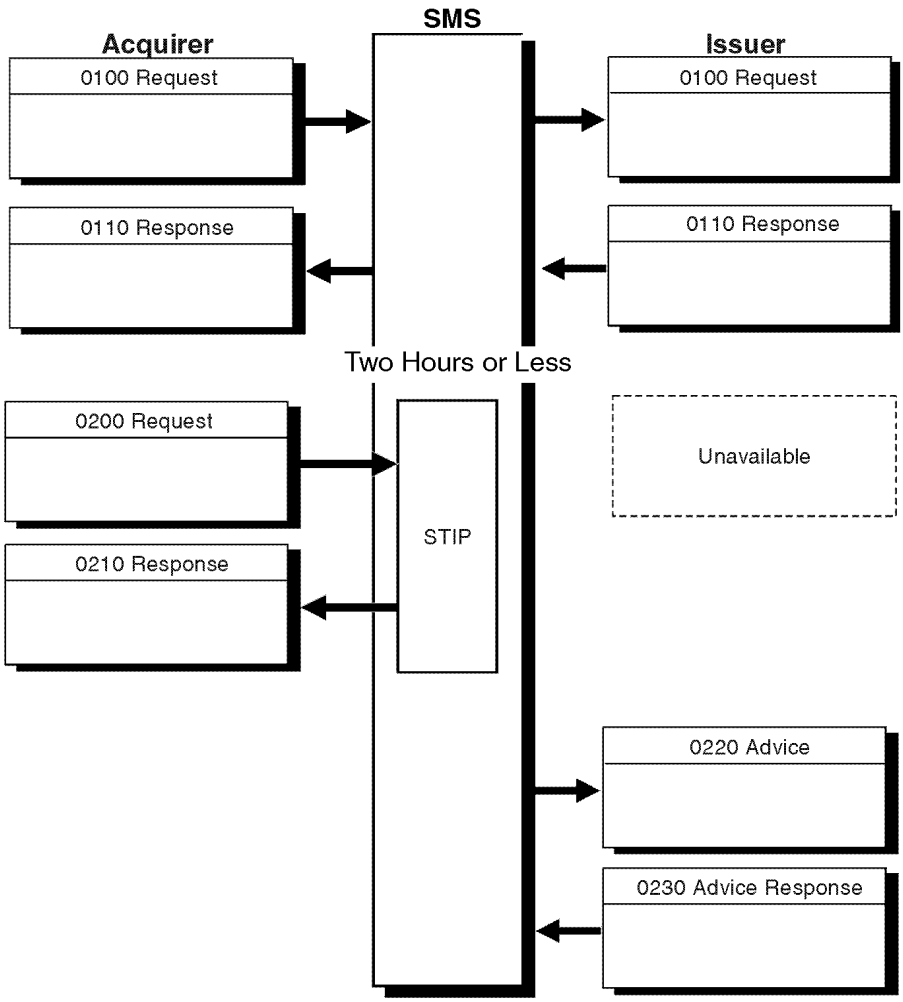
Figure 4–24: Preauthorization Transaction Flow—Issuer Unavailable



Preauthorization—Issuer Unavailable for Preauthorization Completion

The acquirer sends the preauthorization performed while the issuer is available, and the preauthorization completion request (0200) occurs while the issuer is unavailable. STIP authorizes the completion request and stores an advice (0220) for recovery by the issuer. Figure 4–25 illustrates the preauthorization completion transaction flow that occurs when the issuer is unavailable.

Figure 4–25: Preauthorization Completion Transaction Flow—Issuer Unavailable



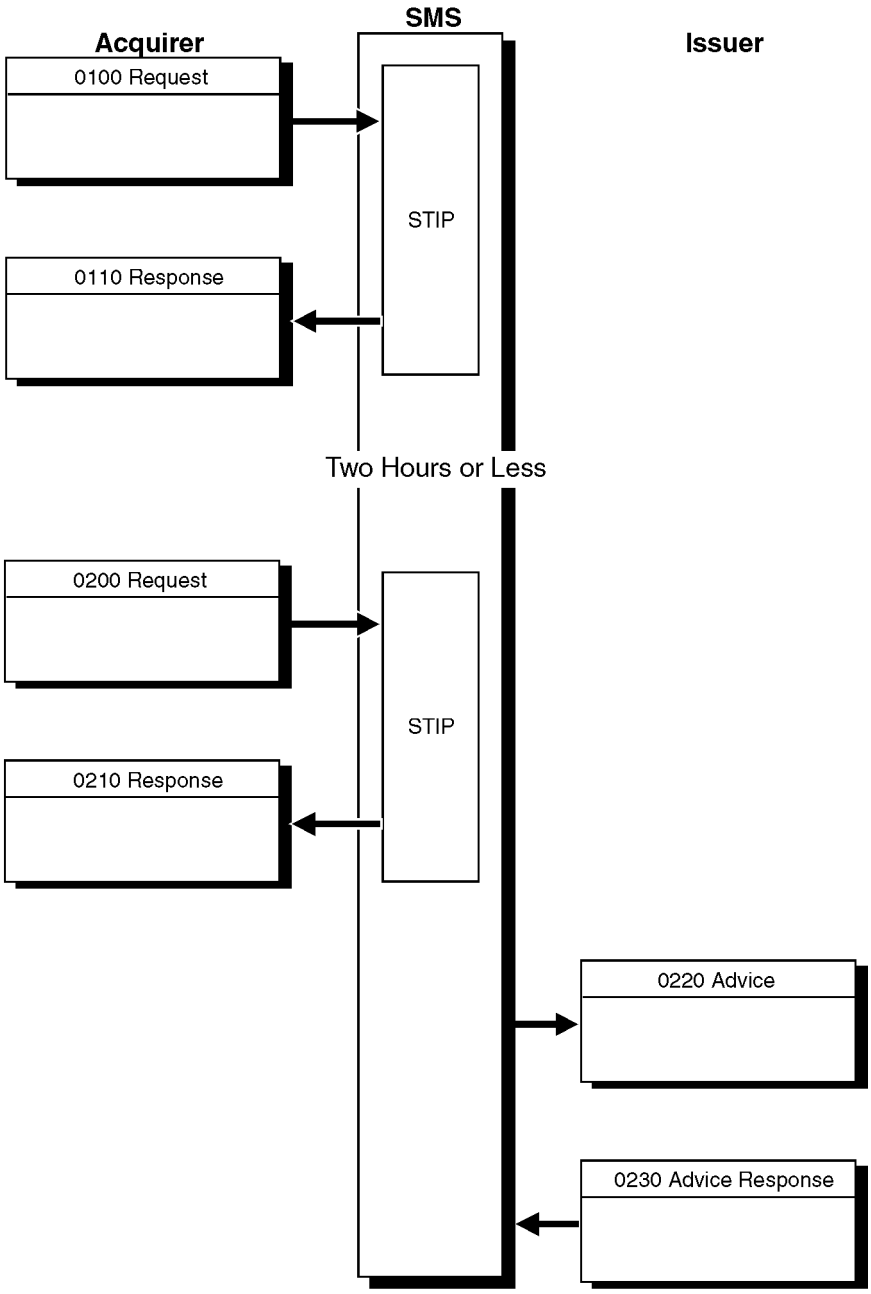
Preauthorization—Issuer Participates in Preauthorization Stand-In Service

For a preauthorization request, STIP sends an 0110 response to the acquirer indicating the stand-in action taken. STIP does not create an 0120 preauthorization advice for the issuer because the issuer participates in Preauthorization Stand-In Service.

For the preauthorization completion request, STIP matches the request to the previously received preauthorization request, and returns an 0210 message to the acquirer. STIP sends an 0220 advice to the issuer, and the issuer acknowledges it with an 0230 message.

Figure 4–26 illustrates the preauthorization transaction flow when the issuer participates in Preauthorization Stand-In Service.

Figure 4–26: Preauthorization Transaction Flow—Issuer Participates in Preauthorization Stand-In Service

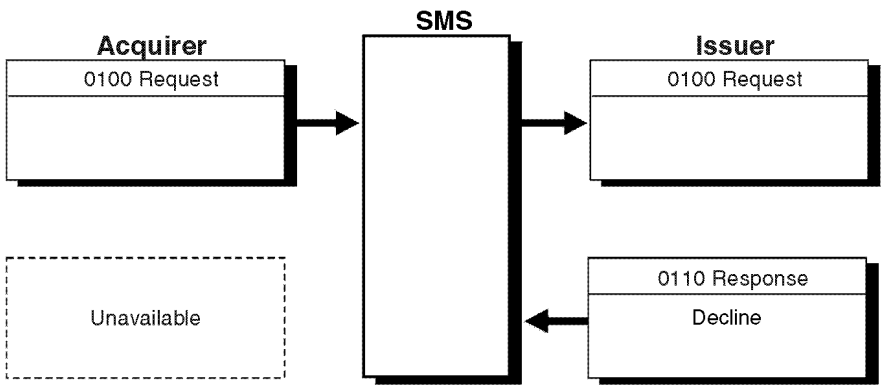


Preauthorization—Acquirer Unavailable After Preauthorization Request—Request Declined

The acquirer becomes unavailable after sending the preauthorization request message (0100) and before receiving the decline response. STIP does not advise the acquirer of the decline because there is no financial impact.

Figure 4–27 illustrates the preauthorization transaction flow for an acquirer that is unavailable after the preauthorization request is declined.

Figure 4–27: Preauthorization Transaction Flow—Acquirer Unavailable After Preauthorization Request; Request Declined

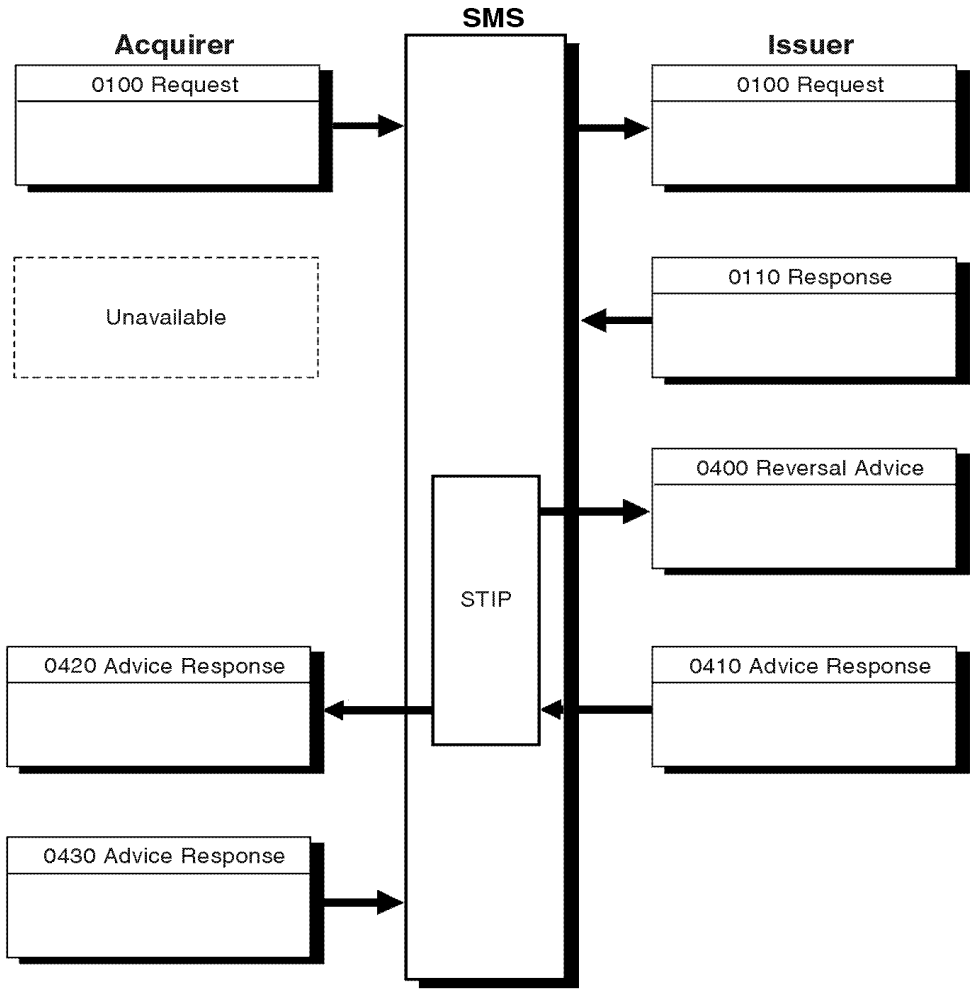


Preauthorization—Acquirer Unavailable After Preauthorization Request—Request Approved

The acquirer becomes unavailable after sending the preauthorization request (0100) and before receiving the approval response. STIP sends an 0400 reversal to the issuer and an 0420 reversal advice to the acquirer. Acquirers are required to submit reversals if they time out.

Figure 4–28 illustrates the preauthorization transaction flow for an acquirer that is unavailable when the preauthorization request is approved.

Figure 4–28: Preauthorization Transaction Flow—Acquirer Unavailable After Preauthorization Request; Request Approved



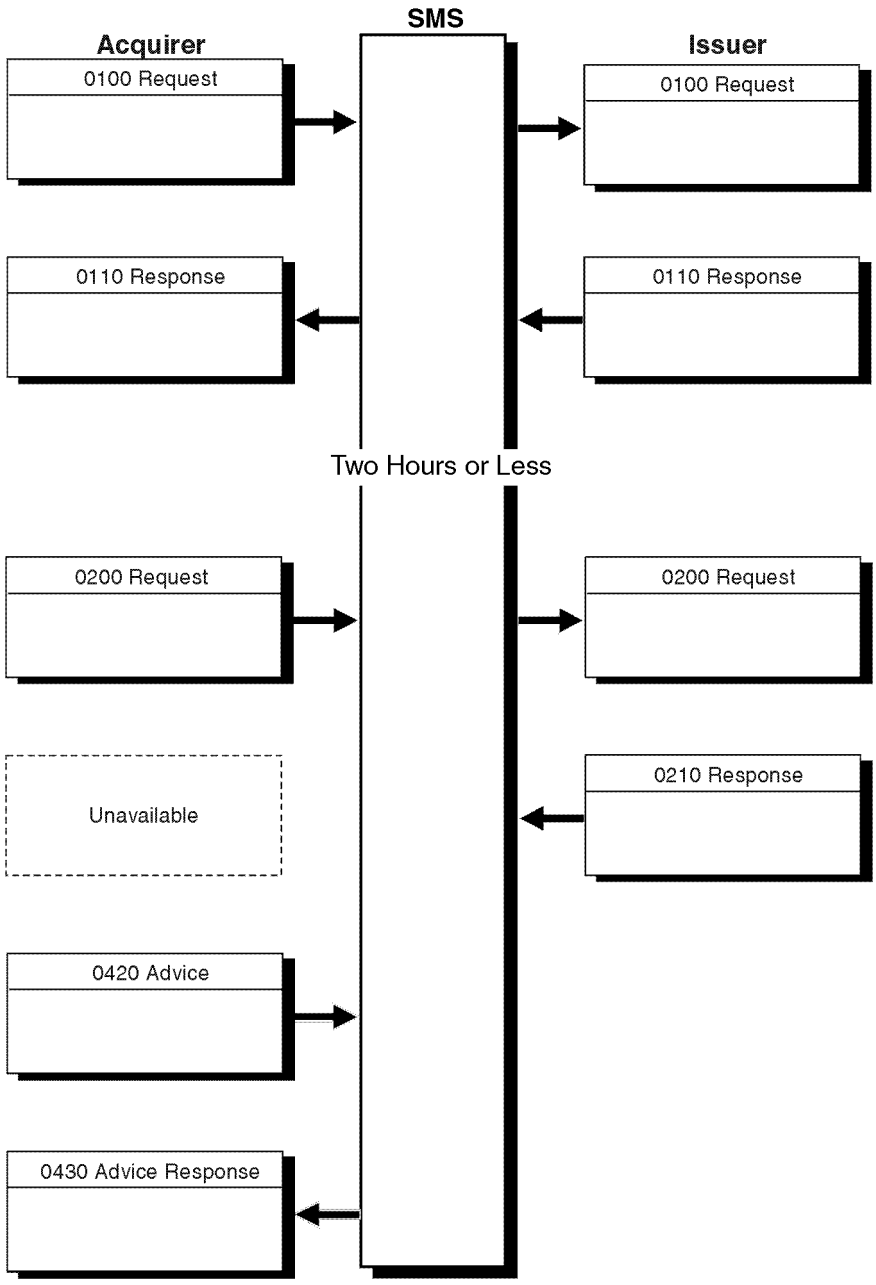
Preauthorization—Acquirer Unavailable After Preauthorization Completion Request; Completion Request Declined

The acquirer becomes unavailable after sending the preauthorization completion request (0200) and before receiving a decline response. STIP does not advise the acquirer of the decline because there is no financial impact.

When the acquirer becomes available, it sends a reversal advice because it is not aware that the request was declined. This advice has no settlement impact because the message the acquirer reverses was already declined.

Figure 4–29 shows the transaction flow for an acquirer that is unavailable when the preauthorization completion request is declined.

Figure 4–29: Preauthorization Transaction Flow—Acquirer Unavailable After Preauthorization Completion Request; Completion Request Declined



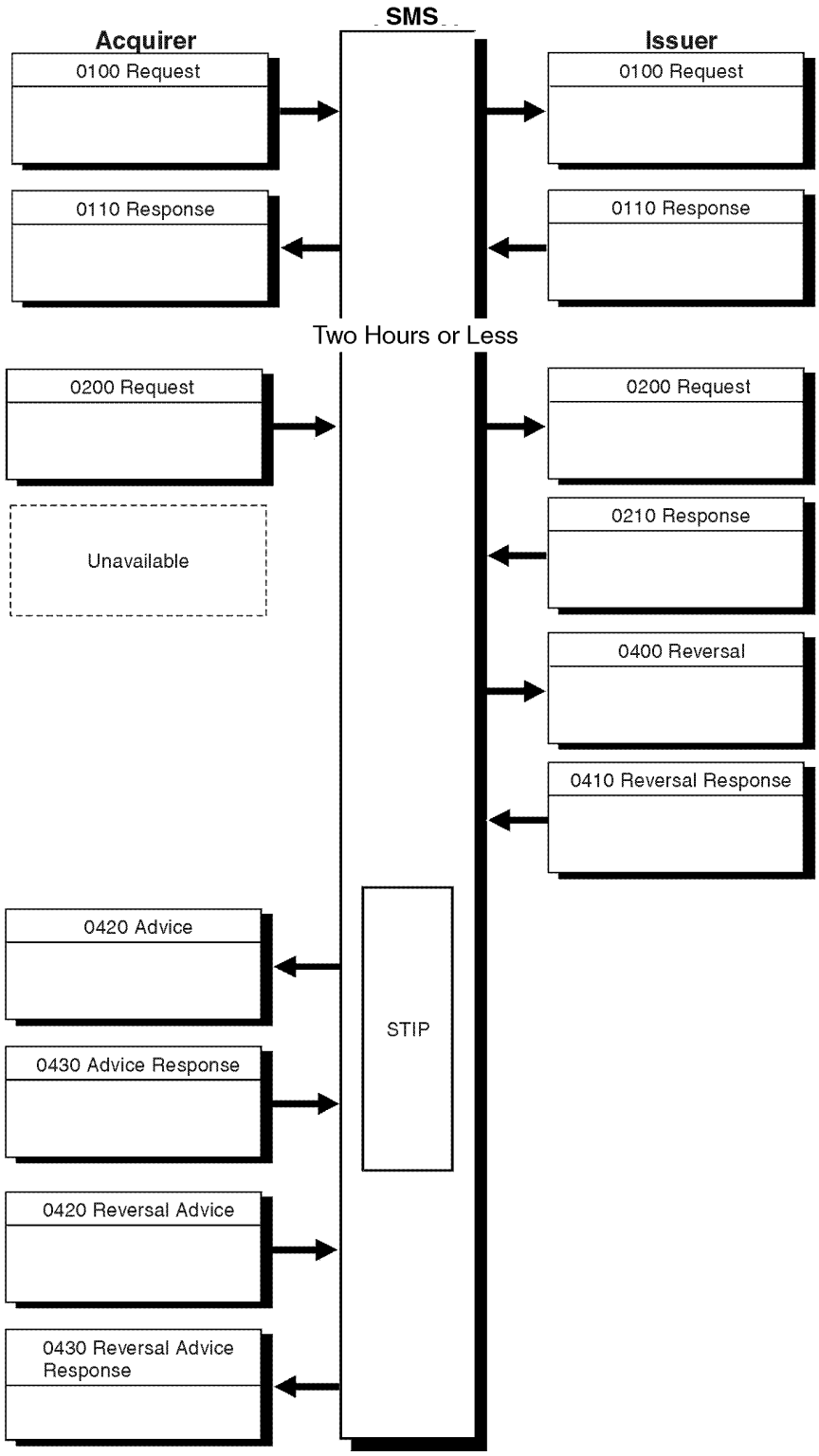
Preauthorization—Acquirer Unavailable After Preauthorization Completion Request; Completion Request Approved

The acquirer becomes unavailable after sending the preauthorization completion request (0200) and before receiving the approval response. STIP sends an 0400 reversal to the issuer and an 0420 reversal advice to the acquirer.

Unless the acquirer has already received an advice from SMS, the acquirer should send an 0420 reversal advice because it did not receive the 0210 response. It receives a response indicating the transaction has already been reversed.

Figure 4–30 illustrates the preauthorization completion request flow for an acquirer that is unavailable when the completion request is approved.

Figure 4–30: Preauthorization Transaction Flow—Acquirer Unavailable After PreauthorizationCompletionRequest;CompletionRequestApproved

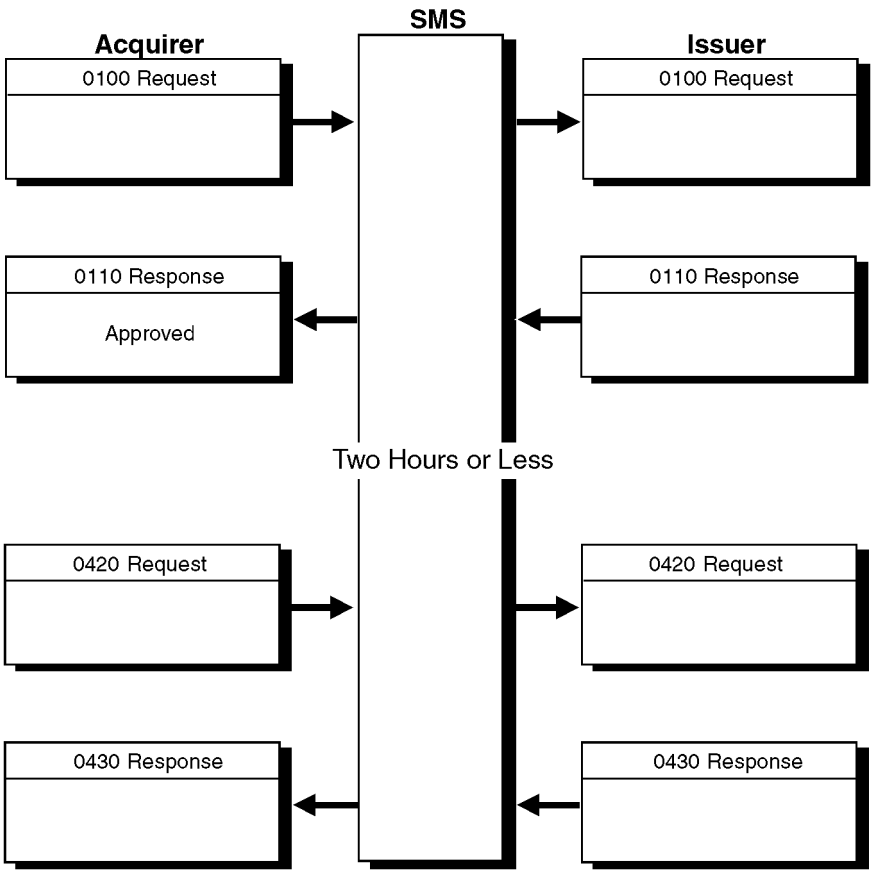


Preauthorization—Acquirer Receives Reversal From Merchant After Preauthorization

The acquirer receives a reversal from the merchant after the preauthorization request (0100) was approved. Acquirers are required to submit a reversal (0420) if the preauthorization is approved and the cardholder decides not to complete the sale or systems conditions prevent completion of the sale. Issuers use reversals to cancel an approved preauthorization.

Figure 4–31 illustrates the preauthorization request transaction flow for a cancellation reversal.

Figure 4–31: Cancellation (Reversal) of Preauthorization Request Transaction Flow



Acquirer or SMS Unavailable After Completion of Preauthorization Request

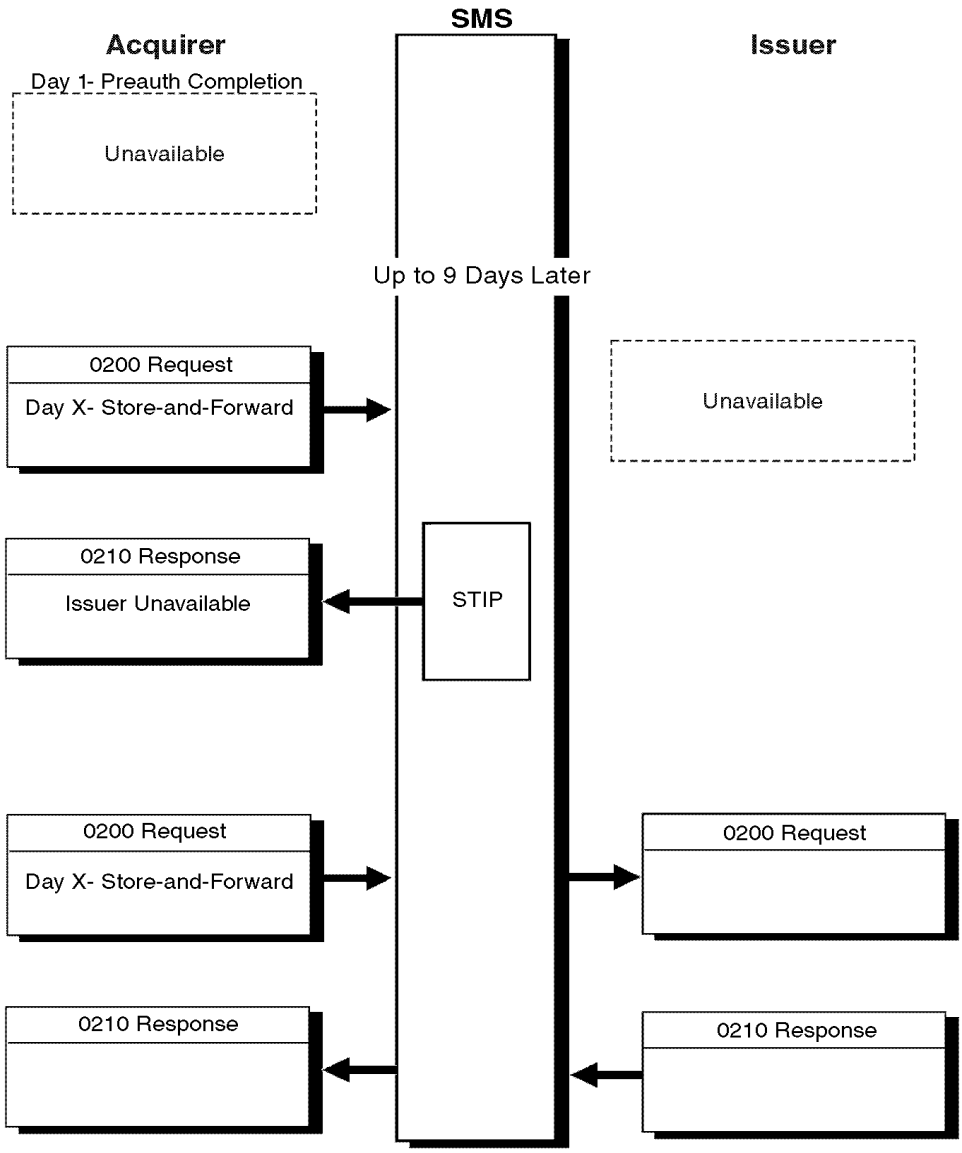
If the merchant cannot send the preauthorization completion within the two-hour period because the acquirer or SMS is unavailable, the merchant should transform the preauthorization completion into a store-and-forward transaction.

Store-and-forward transaction processing provides the acquirer additional opportunity to collect funds on the transaction when system problems occur between the preauthorization request and the preauthorization completion.

If the two-hours-or-less time limit is exceeded, SMS sends the 0200 transaction to the issuer if the issuer is available. If the issuer is not available, SMS puts Response Code 91—Issuer Unavailable in Field 39—Response Code in the 0210 response to the acquirer. SMS does not create an advice for the issuer. An acquirer receiving Response Code 91—Issuer Unavailable should retry the transaction later.

Figure 4–32 illustrates the purchase debit store-and-forward transaction flow.

Figure 4–32: Purchase Debit Store-and-Forward Transaction Flow



Financial Transactions

Exception conditions for financial transactions include the following situations:

- Issuer unavailable
- Issuer unavailable and account on Exception File
- Issuer fails to respond
- Issuer responds late
- Approval cannot be delivered to acquirer
- Decline cannot be delivered to acquirer

Issuer Unavailable

If the issuer is unavailable, STIP responds to the 0200 request and creates an 0220 advice for the issuer to recover. This advice reflects both the request and the STIP reply. When the issuer recovers the 0220 advice, it acknowledges with an 0230 advice response.

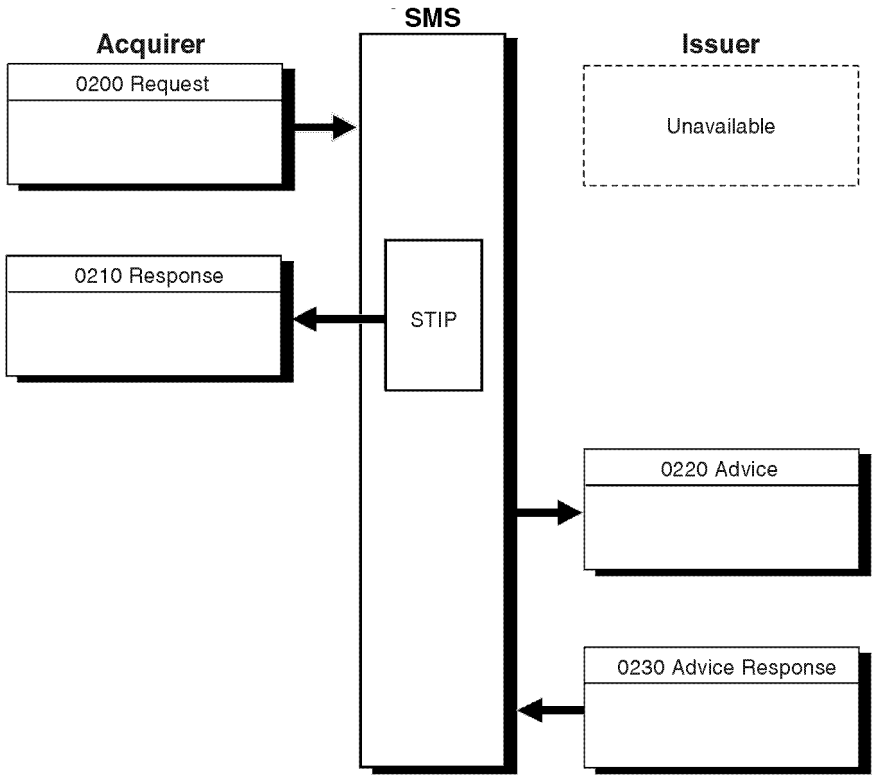
The 0220 advice delivers the transaction to the issuer for account posting. It reflects the acquirer's request and STIP response.

For ATM, SMS responds with Response Code 91—Destination Unavailable in Field 39—Response Code if the 0200 request was for a balance inquiry.

For Interlink, SMS responds with Response Code 91—Destination Unavailable in Field 39—Response Code if the 0200 request was for a balance inquiry, merchant-authorized transaction (store-and-forward transaction or paper sales draft), or resubmission.

Figure 4–33 illustrates stand-in processing for an issuer that is unavailable to send a response to an acquirer's authorization request.

Figure 4–33: Issuer Unavailable Transaction Flow



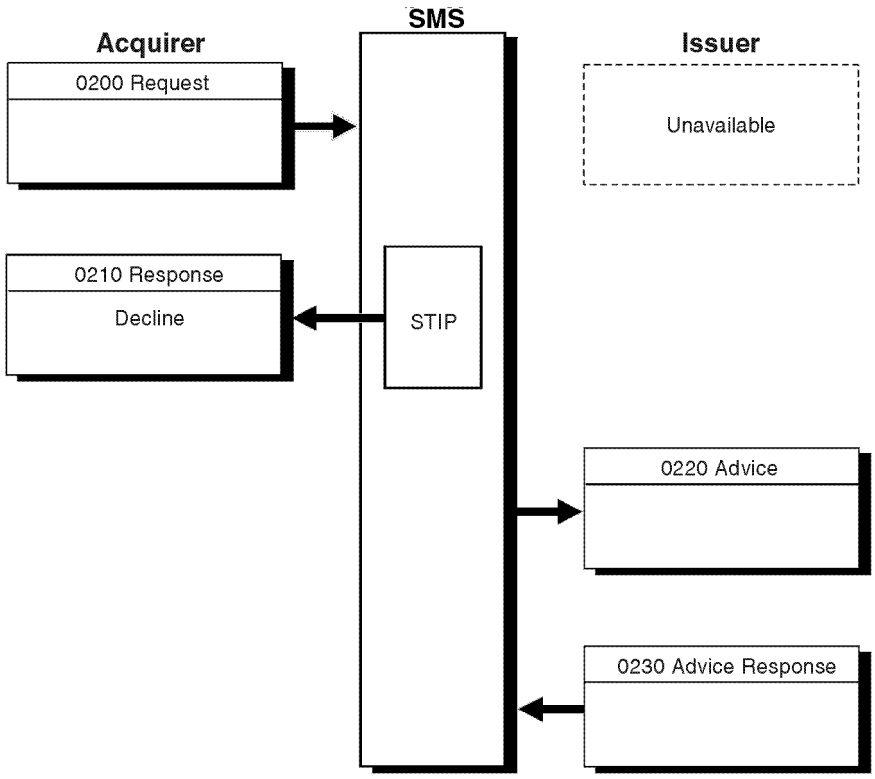
Issuer Unavailable—Account Listed on Exception File

If the issuer is unavailable and the account is listed on the Exception File with a decline, STIP returns a decline response to the acquirer and stores an 0220 advice for the issuer to recover. When the issuer recovers the advice, it acknowledges with an 0230 advice response.

This type of exception condition processing does not apply to ATM.

Figure 4–34 illustrates stand-in processing for an issuer that is unavailable to respond to an authorization request regarding a cardholder account that is listed on the Exception File. The issuer acknowledges the STIP advice when it becomes available to recover it.

Figure 4–34: Issuer Unavailable—Account Listed On Exception File Transaction Flow



This flow provides only one example of STIP exception conditions. STIP also can decline for PIN verification errors or for activity limit exceeded. It can approve if the card involved appears on the Exception File as having VIP (very important person) status.

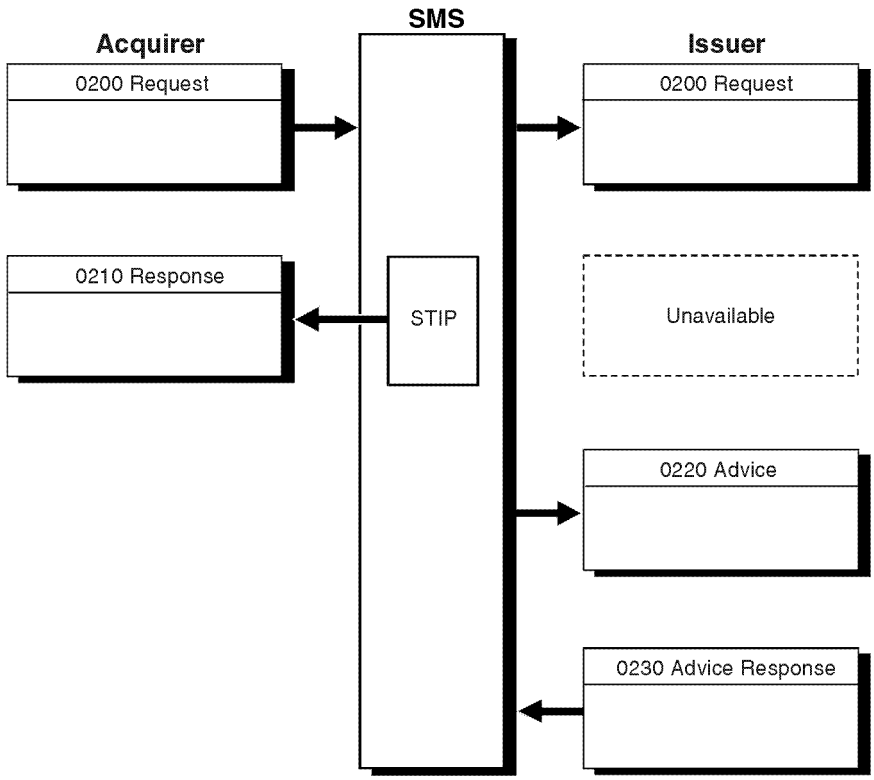
If an issuer participates in the Automatic Cardholder Database Update service (Auto-CDB), the cardholder records in the Exception File are updated when an issuer responds with a response code indicating “pickup card.” This feature facilitates the file maintenance function.

Issuer Fails to Respond

If an issuer receives a request and then becomes unavailable and fails to respond within the required time limit, SMS times out the issuer and passes the transaction to STIP. The 0220 advice notifies the issuer that STIP has responded to the financial request on the issuer's behalf.

Figure 4–35 illustrates STIP standing in when the issuer has received the request but is unable to respond before a time-out has occurred.

Figure 4–35: Issuer Fails to Respond Transaction Flow



Issuer Responds Late

If an issuer is available but does not respond within the required time limit, SMS times out the issuer and sends the transaction to STIP. STIP processes the transaction on behalf of the issuer and sends an 0210 response to the acquirer. Simultaneously, SMS sends an 0220 advice to the issuer.

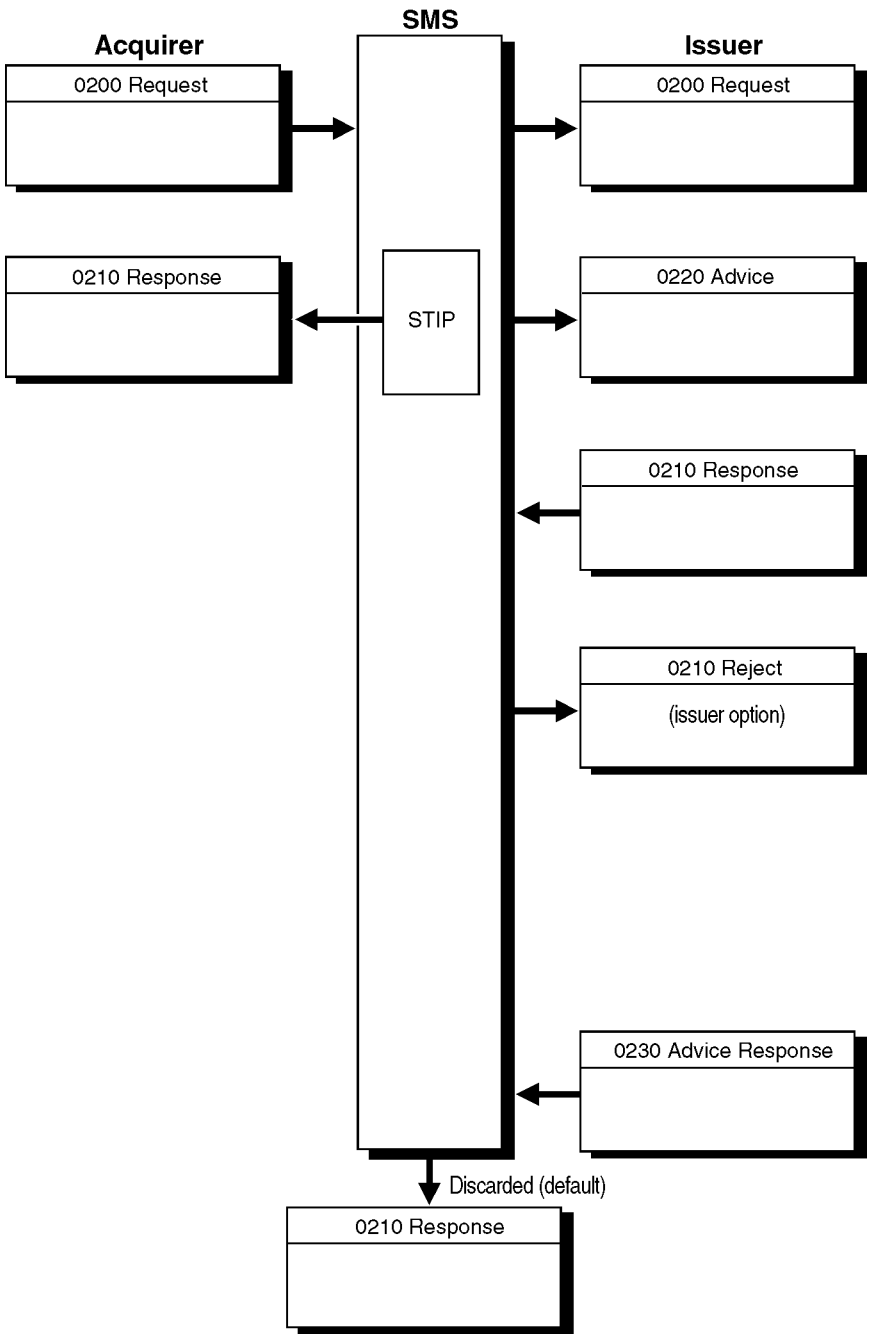
When SMS receives an 0210 response from the issuer *after* the transaction has already been processed by STIP, SMS will do one of the following:

- Reject the 0210 response with a reject code of 515 (late response) in the reject header. This is an issuer-selected option.
- Discard the 0210 response. This is the default option.

Because the 0220 advice is approved or denied based on the issuer's parameters, the STIP financial impact to the cardholder's account may be different than that of the issuer's 0210 response.

Figure 4–36 illustrates STIP standing in when the issuer has received the request but responds late.

Figure 4–36: Issuer Responds Late Transaction Flow



Approval Response Cannot Be Delivered to the Acquirer

If SMS cannot return an 0210 approval response to the acquirer because the acquirer is unavailable, SMS reverses the transaction by creating an 0420 advice that is immediately sent to the issuer, and creates and stores an 0420 advice for the acquirer to recover. When the acquirer recovers the advice, it responds with an 0430 acknowledgment.

Unless the acquirer has already received a reversal advice from SMS, the acquirer should send an 0420 reversal advice to SMS after determining that an 0210 response has not been received.

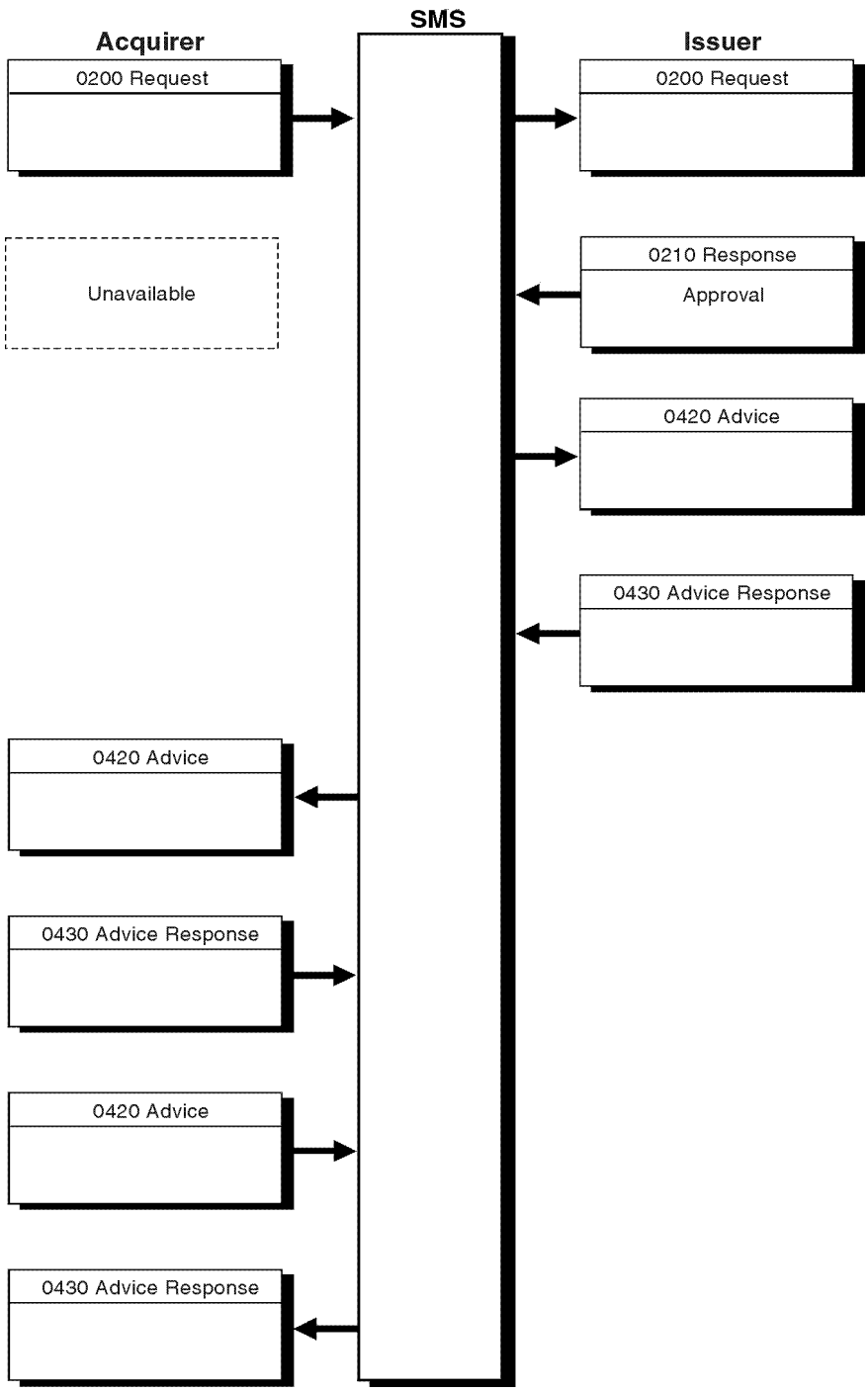
The acquirer should send the 0420 reversal advice because there is no way for the acquirer to know whether SMS reversed the 0200 or whether the 0210 approval response simply never made it back to the acquirer's system in time.

If SMS has not reversed the 0200 already, then the acquirer's 0420 will be treated like a normal reversal and will go through to the issuer.

SMS returns an 0430 response with a response code indicating the transaction has already been reversed.

Figure 4–37 illustrates the transaction flow of an approval that cannot be delivered to the acquirer.

Figure 4–37: Approval Response Cannot Be Delivered to the Acquirer Transaction Flow



Decline Response Cannot Be Delivered to the Acquirer

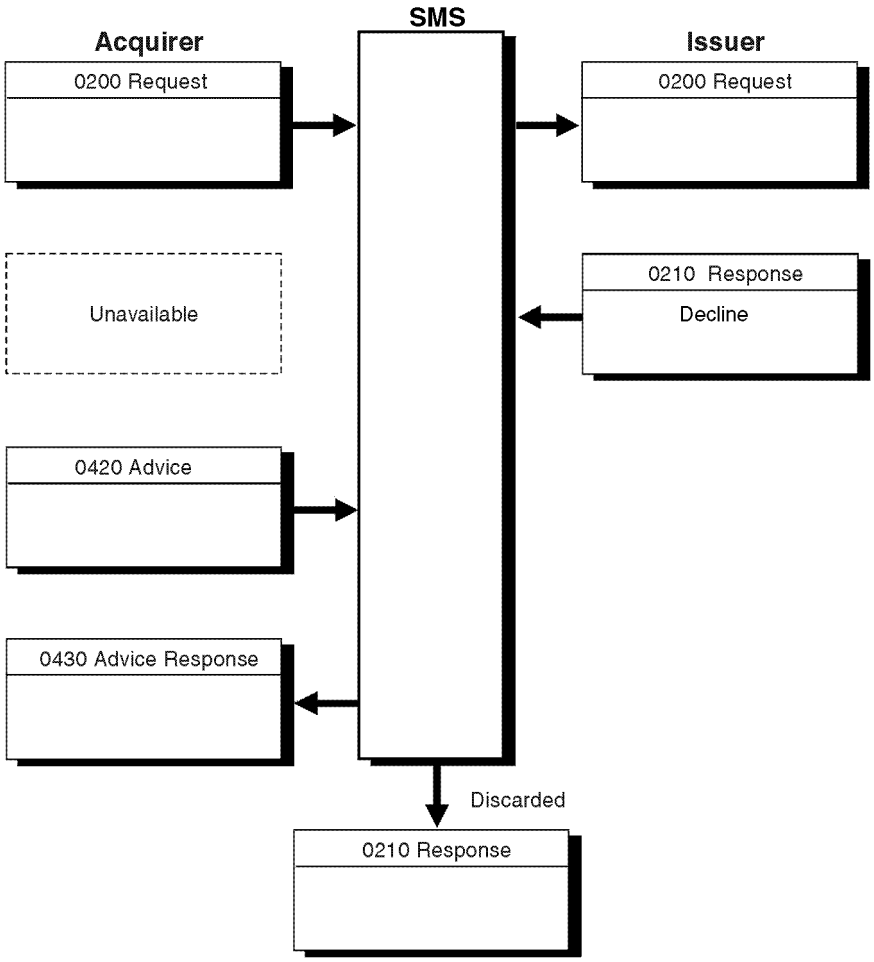
If SMS cannot return an 0210 decline response to the acquirer because the acquirer is unavailable, SMS logs and discards the undeliverable 0210 response.

The acquirer must send an 0420 reversal advice to SMS after determining that an 0210 response has not been received. SMS acknowledges with an 0430 advice response that contains an approval response code. SMS also sets the Gross Interchange Value (GIV) Update Flag to zero, indicating that the reversal has no financial impact.

Because the 0200 message was declined, further messages to the issuer are not necessary.

Figure 4–38 illustrates the transaction flow of a decline response that cannot be delivered to the acquirer.

Figure 4–38: Decline Response Cannot Be Delivered to the Acquirer Transaction Flow



Reversals

There are three types of reversal transactions:

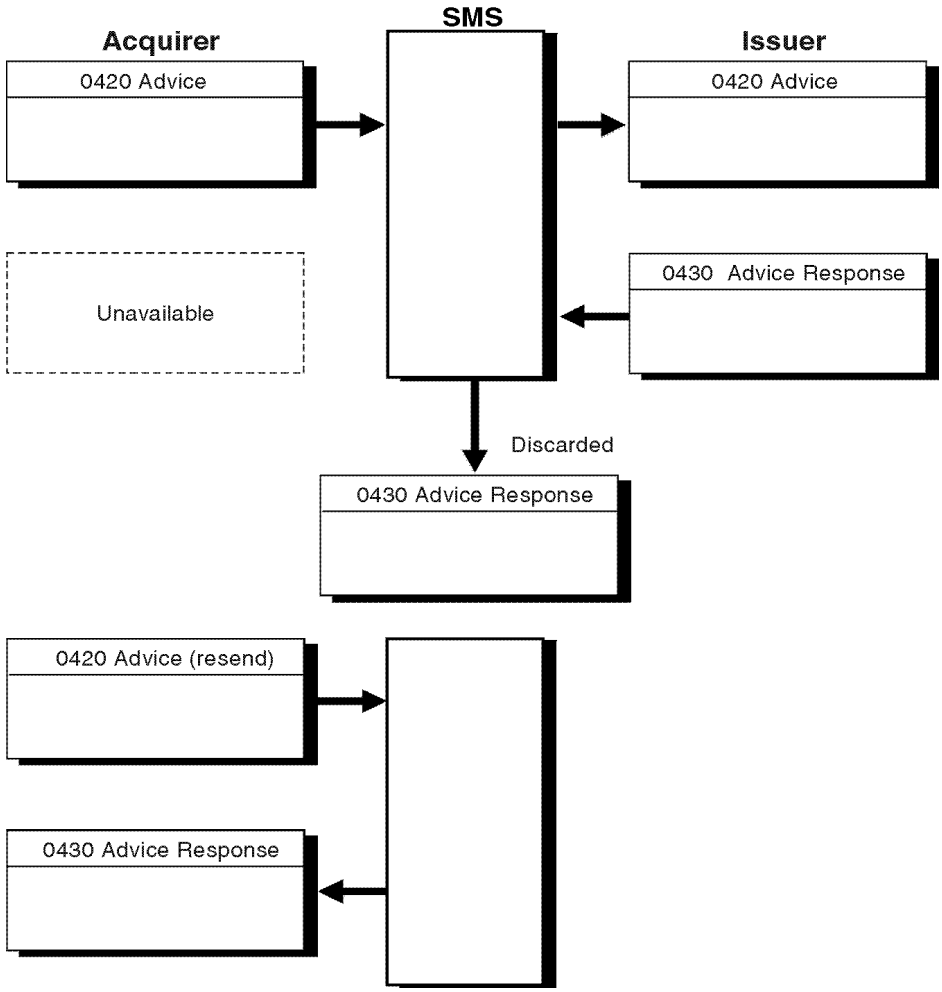
- Reversal advice response cannot be delivered to acquirer
- Reversal with issuer unavailable
- Reversal that is unsolicited

Reversal—Advice Response Cannot Be Delivered to the Acquirer

If SMS cannot forward an 0430 advice response to the acquirer because the acquirer is unavailable, SMS logs and discards the advice response. When the acquirer becomes available, it must resend the 0420 advice. SMS acknowledges with an 0430 advice response.

Figure 4–39 illustrates the transaction flow of an advice that cannot be delivered to the acquirer.

Figure 4–39: Reversal—Advice Response Cannot Be Delivered to the Acquirer Transaction Flow

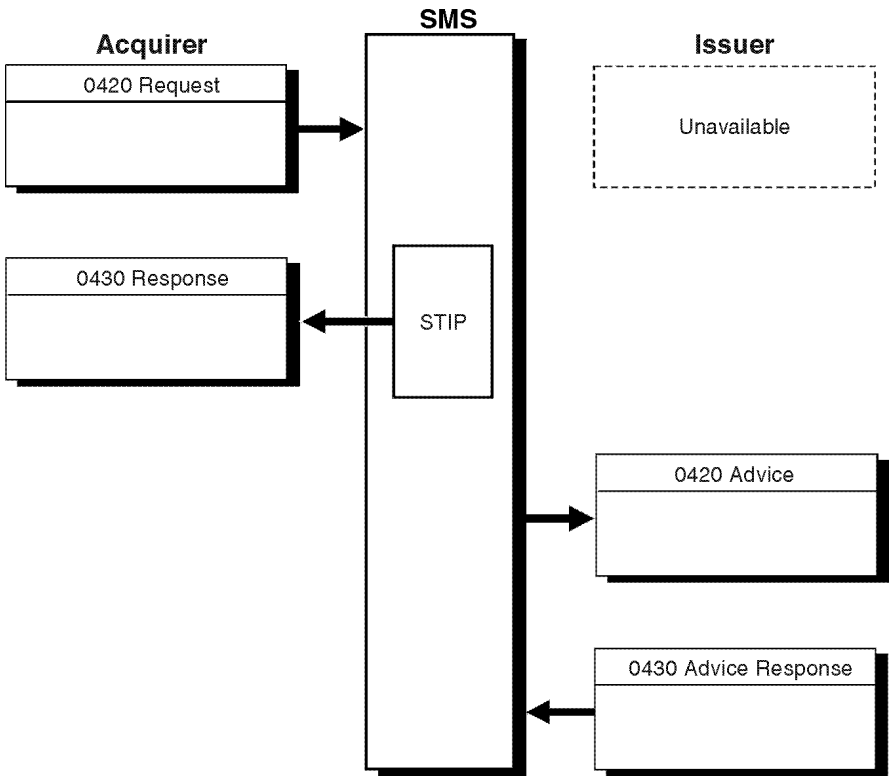


Reversal—Issuer Unavailable

If the issuer times out or is unavailable, SMS responds to the acquirer, then stores an 0420 advice for recovery by the issuer. The issuer acknowledges with an 0430 response.

Figure 4–40 illustrates the transaction flow of a reversal when the issuer is not available.

Figure 4–40: Reversal—Issuer Unavailable Transaction Flow

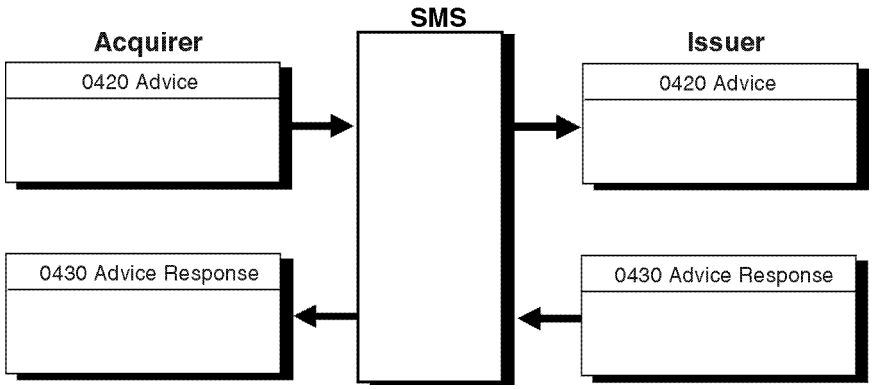


Reversal—Unsolicited

If SMS receives an 0420 reversal request that does not match an earlier financial transaction, SMS approves the request as a nonfinancial transaction (by using the GIV—Gross Interchange Value—flag in header field 5) and responds to the acquirer with an 0430 response message. It then stores an 0420 advice for recovery by the issuer. The issuer acknowledges with an 0430 advice response. The transaction has no financial impact.

Figure 4–41 illustrates the transaction flow for an unsolicited reversal.

Figure 4–41: Reversal—Unsolicited Transaction Flow



Exception Transactions

The following exception transactions include STIP and some other transaction processing performed when either the issuer or acquirer is unavailable.

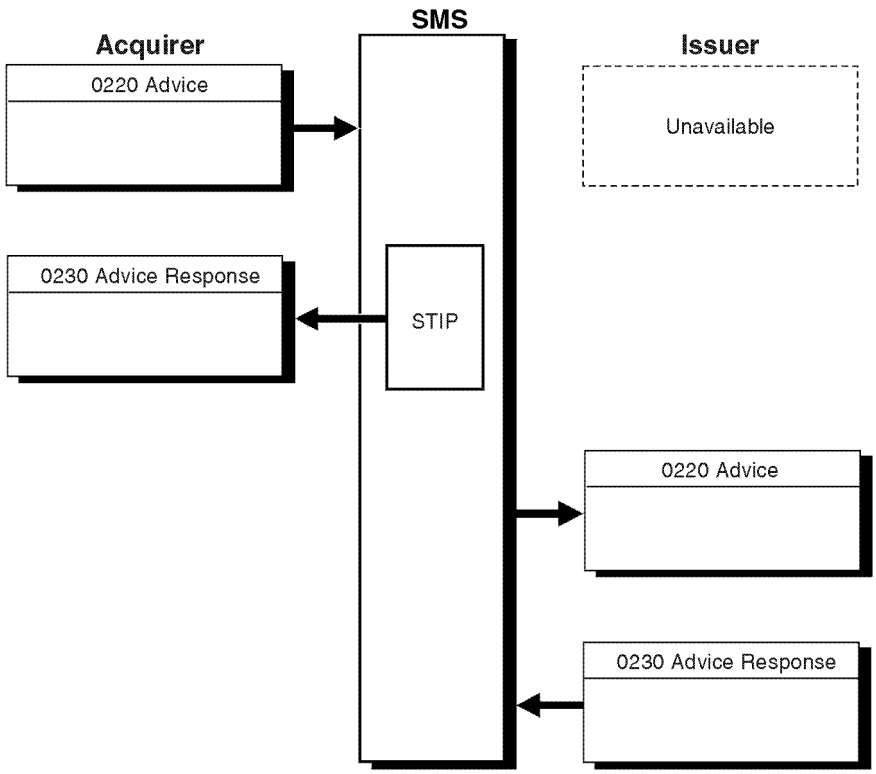
Adjustment or Representment—Issuer Unavailable

If the issuer is unavailable, STIP authorizes the adjustment or representment advice and responds to the acquirer. STIP builds and stores an 0220 advice for issuer recovery.

This processing includes Interlink good faith collections.

Figure 4–42 illustrates an adjustment or representment transaction flow when the issuer is unavailable.

Figure 4–42: Adjustment or Representment—Issuer Unavailable Transaction Flow



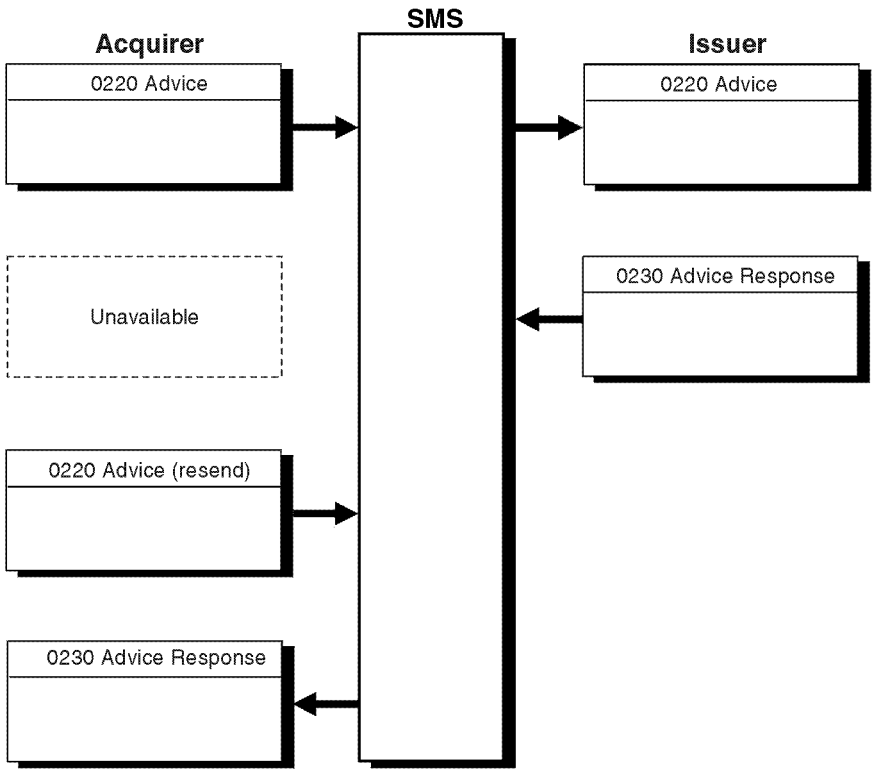
Adjustment or Representment—Acquirer Unavailable After Advice

If the acquirer becomes unavailable after sending the adjustment or 0220 representment advice and cannot receive the response, the acquirer must resend the 0220 advice unchanged. SMS recognizes the duplicate advice and generates a response to the acquirer as though the duplicate advice were the original.

This processing includes Interlink good faith collections.

Figure 4–43 illustrates an adjustment/representment transaction flow when the acquirer is unavailable.

Figure 4–43: Adjustment or Representment—Acquirer Unavailable Transaction Flow

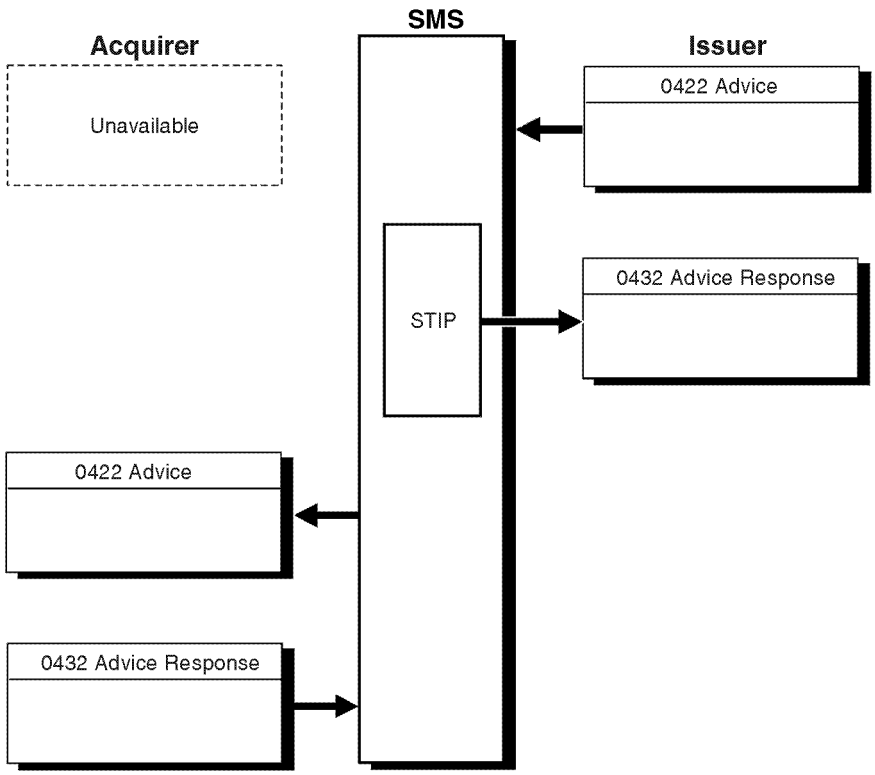


Chargeback—Acquirer Unavailable

If the acquirer is unavailable when the issuer sends a chargeback, STIP accepts the transaction, responds to the issuer, and builds and stores the chargeback advice for the acquirer to recover.

Figure 4–44 illustrates STIP authorizing a chargeback.

Figure 4–44: Chargeback—Acquirer Unavailable

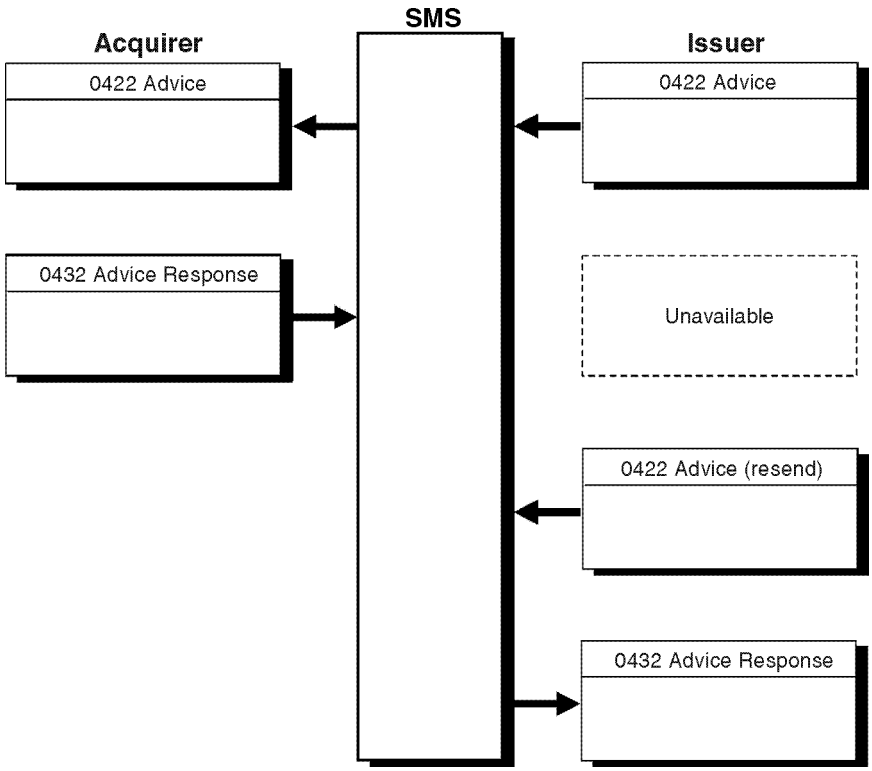


Chargeback—Issuer Unavailable After Chargeback

If the issuer becomes unavailable after sending an 0422 chargeback advice and before receiving the response, the issuer must resend the chargeback unchanged. Upon receiving the resent 0422 advice, SMS recognizes that the original request was processed and forwards to the issuer the 0432 advice received from the acquirer in response to the original request.

Figure 4–45 illustrates the transaction flow of an issuer unavailable after a chargeback.

Figure 4–45: Chargeback—Issuer Unavailable After Chargeback Transaction Flow



Multicurrency Support 5

Participation in the Multicurrency Service is a requirement for Interlink members outside of the United States (U.S.) region.

V.I.P. SingleConnect POS Service features full *multicurrency support* for international Interlink transactions. Interlink multicurrency support includes:

- Automatic conversion from the transaction currency to the currency of the cardholder's account
- Automatic conversion from the transaction currency to the acquirer's settlement currency (if the two are different)
- Automatic conversion from the currency of the cardholder's account to the issuer's settlement currency (if the two are different)

The *transaction currency* is generally the currency of the country in which a transaction takes place. The acquirer indicates the transaction currency in the Interlink message.

The *cardholder billing currency* is generally the currency of the country in which the account is domiciled. SMS determines the currency of a cardholder's account from the issuer's BIN of the Primary Account Number (PAN) on the card's magnetic stripe.

The Multicurrency Service provides expanded currency information in online messages, on reports, and in raw data.

SMS messages contain several multicurrency fields supporting the various amounts involved in currency exchange calculation. These fields contain the following data:

- The transaction amount in the transaction currency
- The transaction amount in the cardholder billing currency
- The settlement amount
- The conversion rates
- The date of the conversion rate table used by SMS

Participating members receive these standard multicurrency fields in their online messages, reports, and raw data.

For nonparticipating members, transaction and settlement amounts appear in online messages, raw data, and reports in U.S dollars only. Nonparticipating members that migrate to the Multicurrency Service have the advantage of using the additional information.

Currencies

SMS determines applicable currencies for a given transaction as follows:

- The acquirer indicates the transaction amount and the transaction currency in the request message. The transaction currency is generally the currency of the country in which a transaction takes place.
- SMS determines the issuer's currencies based on the first several digits of the PAN, which is read from the magnetic stripe on the card used for the transaction. These initial digits, called the BIN, are used to locate issuer-supplied data, including the *cardholder billing currency* and the *issuer's settlement currency,* on SMS databases.
- SMS determines the *acquirer's settlement currency* based on the acquirer ID in the request message. This ID is used to locate acquirer-supplied data on SMS databases.

SMS supports transaction and cardholder billing currencies recognized by the International Organisation for Standardisation (ISO). Some of these currencies are also supported as settlement currencies. For the current list of supported currencies, see the country and currency codes appendix of the *V.I.P. System SingleConnect Service Interlink Technical Specifications*.

How Currency Conversion Works

There are three components of the currency conversion calculation used by SMS:

1. A base rate (wholesale or government-mandated rate)
2. A Visa currency conversion fee
3. An optional issuer fee (positive or negative percentage)

For example, for converting from U.S. dollars to Hong Kong dollars, the components might be as follows on a given day:

1. Base rate = 7 (that is, 7 Hong Kong dollars for each U.S. dollar)
2. Visa currency conversion fee = 1%
3. Optional issuer fee = .25%

For a transaction of US$100, a cardholder for this issuer would be charged HK$708.75. This is calculated as follows:

1. US$100 x 7 = HK$700.00
2. + Visa 1% = HK$7.00 = HK$707.00
3. + issuer .25% = HK$1.75 = HK$708.75

The wholesale rate is determined daily based on the cost to Visa of buying and selling currencies in the foreign exchange markets. The Visa currency conversion fee for interregional transactions is currently 1%. The Visa currency conversion fee for intraregional transactions can vary by region.

Issuers can elect to charge an optional issuer fee to the cardholder for transactions that require currency conversion. The optional issuer fee is maintained in SMS databases by issuer BINs. This optional fee is calculated at the time of currency conversion using the percentage rate established by the issuer.

The same conversion rates are used in all VisaNet systems that support multicurrency processing.

SMS performs currency conversion in calculating settlement amounts when the acquirer's settlement currency is not the same as the transaction currency or the issuer's settlement currency is not the same as the cardholder billing currency. This currency calculation uses only the base rate.

NOTE: *There is no settlement amount for nonfinancial transactions and currency conversion fees are not charged to the issuer. However, to accurately reflect funds availability, SMS includes conversion fees when it converts balance inquiry amounts for the acquirer.*

What the Issuer Receives

When SMS performs currency conversion, as described in the "How Currency Conversion Works" section of this chapter, the issuer receives the following. (The values are from the same example.)

- The transaction amount and currency code (US$100)
- The cardholder billing amount and currency code (HK$708.75)
- The settlement amount and currency code (HK$700.00)

Another amount, the Visa currency conversion fee (HK$7.00 in this example), is identified in raw data as the Conversion Fee. The settlement amount plus the currency conversion fee is charged to the issuer. The difference between this total and the cardholder billing amount—the optional issuer fee (in this example, HK$1.75)—is revenue for the issuer.

The issuer also receives the currency conversion rate used for the cardholder billing amount, and the currency conversion rate used for the settlement amount.

NOTE: *There is no settlement amount for nonfinancial transactions and currency conversion fees are not charged to the issuer. However, to accurately reflect the account's true buying power, SMS calculates conversion fees when it converts preauthorization and balance inquiry amounts.*

Variations

The effective rate used by SMS to perform currency conversion varies based on the type of transaction:

- For the following transactions, SMS uses the currency conversion procedure described in the "How Currency Conversion Works" section with the current day's base rate plus the Visa currency conversion fee and the optional issuer fee:
  - Purchases and purchases with cashback
  - Preauthorization requests
  - Scrip transactions
  - Adjustments
  - Representments
  - Resubmissions

- For the following transactions, all of which follow an earlier transaction of the same transaction set, SMS *uses the base rate that was in effect at the time of the earlier transaction*, plus the Visa currency conversion fee and the optional issuer fee:

  – Reversal

    If the reversal transaction is initiated within three days of the original transaction, SMS uses the same rate as for the original transaction. If the reversal is initiated more than three days after the original transaction and the new currency rate is not yet available, SMS still uses the same rate as for the original transaction.

  – POS cancellation

    SMS uses the same conversion rate as the transaction being cancelled.

  – Preauthorization completion

    SMS uses the same conversion rate as the preauthorization request.

- For *chargebacks*, SMS uses the base currency conversion rate in effect on the day of the chargeback—without calculating the currency conversion fee and optional issuer fee. The amount of the chargeback in the acquirer's currency is usually the same as the amount of the original transaction.

- For *merchandise credits*, SMS calculates the currency conversion fees and subtracts the fees from the cardholder billing amount.

- For *balance inquiries*, SMS subtracts the currency conversion fee and optional issuer fee from the available balance to reflect the true buying power of the balance amount.

- For a *preauthorization partial amount response* to a preauthorization request, SMS uses the same rates on the partial amount supplied by the issuer, but subtracts the currency conversion fee and optional issuer fee from the amount authorized to reflect the true buying power of the partial amount.

EXAMPLE

In preauthorization partial amount responses and balance inquiries, the currency conversion fees and optional issuer fees are subtracted from the response amount that is passed on to the acquirer. Assuming a base rate of .01 when converting Japanese yen to U.S. dollars, a cardholder's available balance of ¥10,000 is enough for a US$98.75 purchase at the current rate:

1. Available balance = ¥10000 x .01 base rate = US$100.00
2. Less currency conversion fee of 1% = US$1.00 = US$99.00
3. Less issuer fee of .25% = US$0.25 = US$98.75

See the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications* for details on field descriptions and message formats.

Decimal Places in Amounts

Currencies are defined as having zero, two, or three minor units of currency. For example, the U.S. dollar has two minor units of currency (the two positions to the right of the decimal point); the Japanese yen has no minor units.

In online transactions processed by SMS, amounts have an implied decimal point preceding the right-most zero, two, or three digits to handle these minor units of currency. Based upon the currency definition, a numeric value of 6789 is interpreted as 6.789 (three minor units of currency), 67.89 (two minor units of currency), or 6789 (no minor units of currency). The list of currency codes in the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications* indicates the number of implied decimal points in the amount fields.

Although SMS supports up to three significant decimal places in amount fields in online messages, the third digit is assumed to be zero. Therefore, the user of a currency with three decimal places must:

1. Round the amount to a two-place accuracy, or replace the third decimal position with zero when generating amount fields.
2. Be able to receive amounts with two-place accuracy in any amount field supplied by SMS.

For example, the amount 9.246 can be rounded to 9.250, or the third digit can be dropped for a value of 9.240.

Currency Precision Service

Multicurrency Service participants can also participate in the Currency Precision Service, which uses Field 63.13—Decimal Positions Indicator to indicate how many decimal positions are in the message's amount fields. The field accommodates three different values for transaction, settlement, and cardholder amounts. SMS checks them against the Currency Table.
The values allowable in Field 63.13 are shown in Table 5–1.

Table 5–1: Field 63.13 Values

Value	Number of Decimal Positions
00	No decimal positions
01	One decimal position
02	Two decimal positions
03	Three decimal positions
99	Decimal positions do not apply

Adding a Decimal Position

If the number of decimal positions specified in field 63.13 is less than that in the Currency Table, SMS adjusts the applicable amount fields.

EXAMPLE

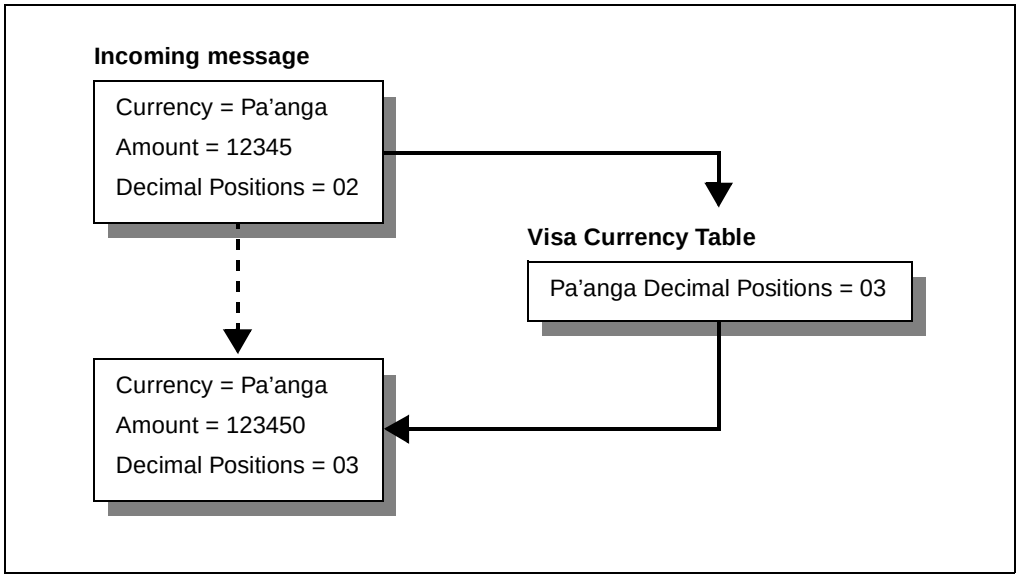
An acquirer sends a transaction amount of 12345 and places 02 in positions 1 and 2 of the Decimal Positions Indicator field. However, the Currency Table indicates that the currency has three decimal positions. Visa reports the amount as 123450 and sends the issuer a transaction amount of 123450.

A participating issuer also receives a Decimal Positions Indicator with 03 in positions 1 and 2 of the field. A nonparticipating issuer receives 123450 in Field 4—Amount, Transaction, but no Decimal Positions Indicator in the request.

The acquirer receives the transaction amount 123450 and 03 in positions 1 and 2 of the Decimal Positions Indicator field. Settlement amount is based on 123450. All reports

and raw data reflect the transaction amount 123450. An example of decimal position conversion—one position is shown in Figure 5–1.

Figure 5–1: Adding a Decimal Position—Conversion Example



Removing a Decimal Position

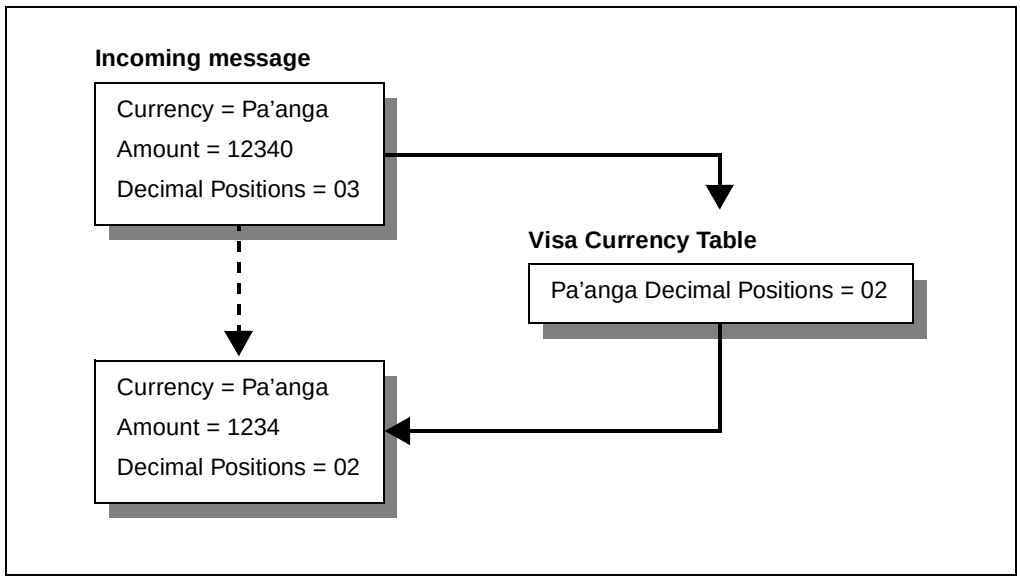
If the number of decimal positions specified in field 63.13 is greater than that in the table, the last digit (which must be zero) is removed.

EXAMPLE

An acquirer sends a transaction amount 12340 with 03 in the transaction amounts subfield of the Decimal Positions Indicator, but the Currency Table indicates the currency has two decimal positions (see Figure 5–2).

The issuer receives 1234. A participating issuer also receives a Decimal Positions Indicator with 02 in the transaction amounts subfield. Nonparticipating issuers receive 1234 but no Decimal Positions Indicator. Settlement amount is based on 1234. All reports and raw data reflect 1234.

Figure 5–2: Removing a Decimal Position—Conversion Example



The Currency Precision Service is only available to SingleConnect participants using the Multicurrency Service.

Members Not Participating in the Multicurrency Service

Although participation in the Multicurrency Service is not currently required for all members, Visa supports currency conversion for all international transactions in that:

- The member that participates in the Multicurrency Service will not be aware that the other member is not receiving the enhanced data fields.
- The U.S. acquirer that does not participate in the Multicurrency Service can optionally receive the country code of the issuer in Field 20—PAN Extended, Country Code.
- The U.S. issuer that does not participate in the Multicurrency Service can identify the country of the acquirer from the value in Field 19—Acquiring Institution Country Code.

Multicurrency Field Flows

This section gives examples of the content and processing of amount-related fields for online multicurrency support. The examples assume that both the acquirer and issuer participate in the Multicurrency Service. In each case, the examples show:

1. The fields the message originator must provide.
2. The processing performed by SMS.
3. The fields forwarded to the message recipient.
4. The fields provided to the originator in the response.

Examples are:

- Preauthorization (0100)
  - Full Approval (Figure 5–3)
  - Partial Approval (Figure 5–4)
- Financial Transactions (0200 and 0220)
  - Preauthorization Completion (Figure 5–5)
  - Purchase Transaction (Figure 5–6)
  - Adjustment (Figure 5–7)
  - Representment (Figure 5–8)
- Balance Inquiry (0200) (Figure 5–9)
- Reversal (0400 and 0420) (Figure 5–10)
- Chargeback (0422)
  - Full Amount (Figure 5–11)
  - Partial Amount (Figure 5–12)
- Merchandise Credit (0200 and 0210) (Figure 5–13)

The amounts contained in reconciliation messages (0500 and 0520) are in the settlement currency of the issuer or acquirer receiving the message. Settlement currencies can differ from the local transaction currency, for an acquirer, and from the cardholder billing currency, for an issuer.

Each example in this section assumes that the merchant does business in Japanese yen and the cardholder is billed in Australian dollars.

The currency codes used are:

036 = Australian dollars

392 = Japanese yen

840 = U.S. dollars

The following fields are used in the multicurrency flows:

Field 4—Amount, Transaction

Field 5—Amount, Settlement

Field 6—Amount, Cardholder Billing

Field 9—Conversion Rate, Settlement

Field 10—Conversion Rate, Cardholder Billing

Field 16—Date, Conversion

Field 39—Response Code

Field 49—Currency Code, Transaction

Field 50—Currency Code, Settlement

Field 51—Currency Code, Cardholder Billing

Field 54—Additional Amounts

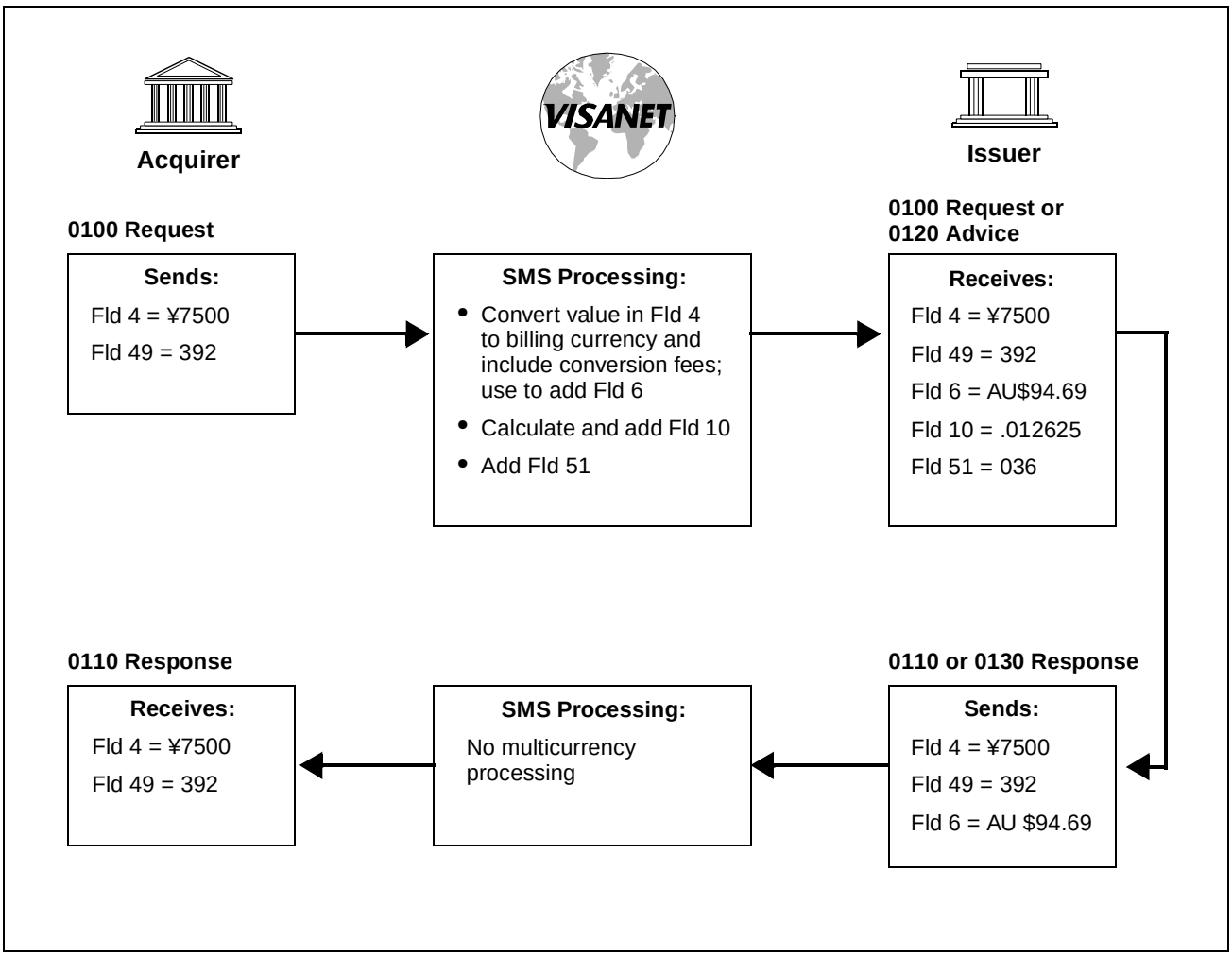
Field 61.1—Other Amount, Transaction

Field 61.2—Other Amount, Cardholder Billing

Field 54 is used for account balance information. It contains the following information for up to four different balance amounts: account type, amount type, currency code, and sign.

The issuer provides account balance information in the first amount field and optionally in the second amount field, both in the cardholder billing currency. SMS converts the first amount and (if present) the second amount to the transaction currency and sends the converted amounts to the acquirer in the third and fourth amount fields, respectively. In the following examples, these amounts are referred to as fields 54A, 54B, 54A-converted, and 54B-converted.

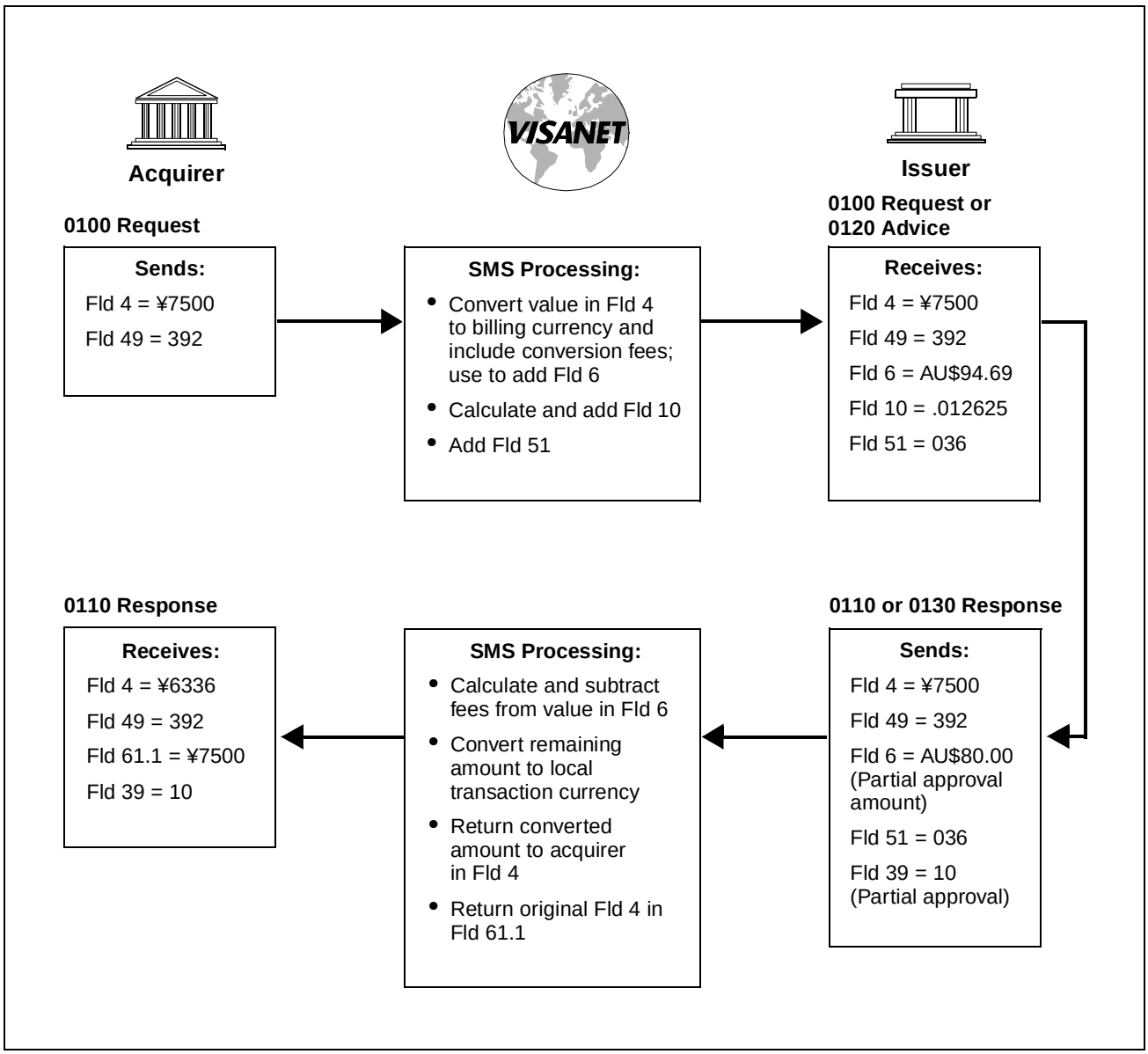
Figure 5–3: Preauthorization—Full Approval



For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

An 0120 advice of an authorization contains the same fields normally received by the issuer in the 0100 message. An 0130 message does not contain field 4 or field 49 because it is an advice message.

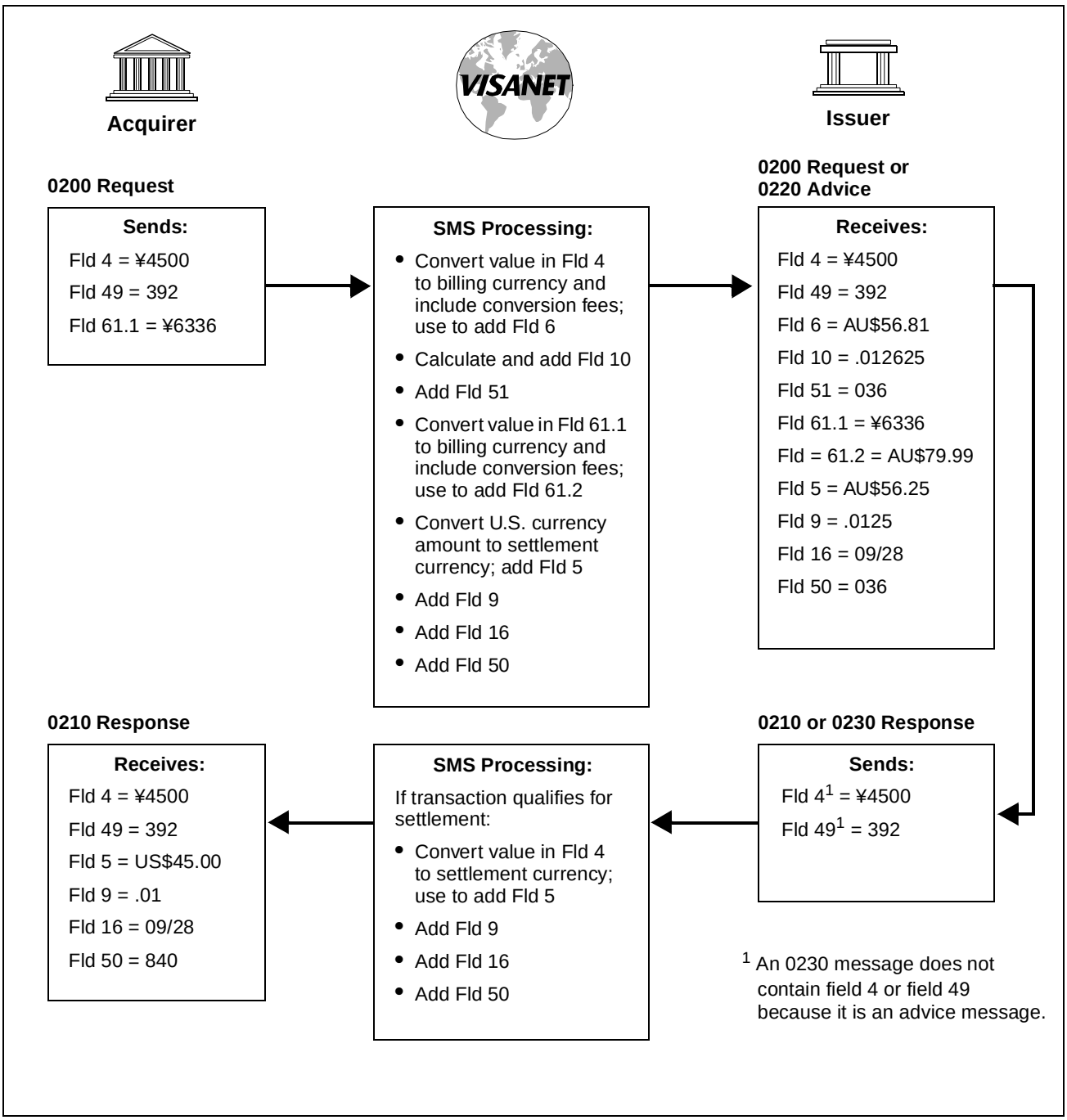
Figure 5–4: Preauthorization—Partial Approval



For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

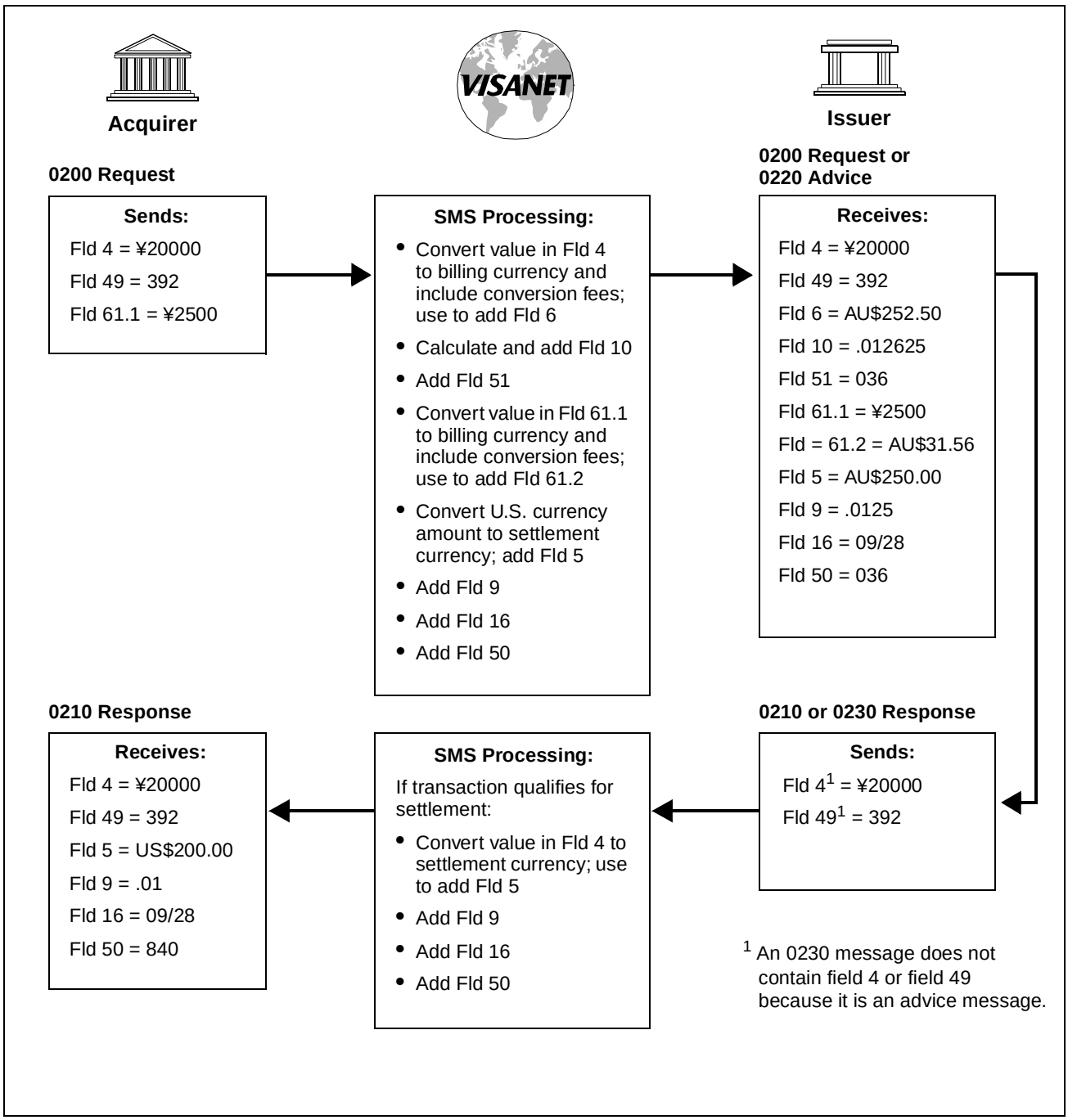
An 0120 advice of an authorization contains the same fields normally received by the issuer in the 0100 message. An 0130 message does not contain field 4 or field 49 because it is an advice message.

Figure 5–5: Preauthorization Completion



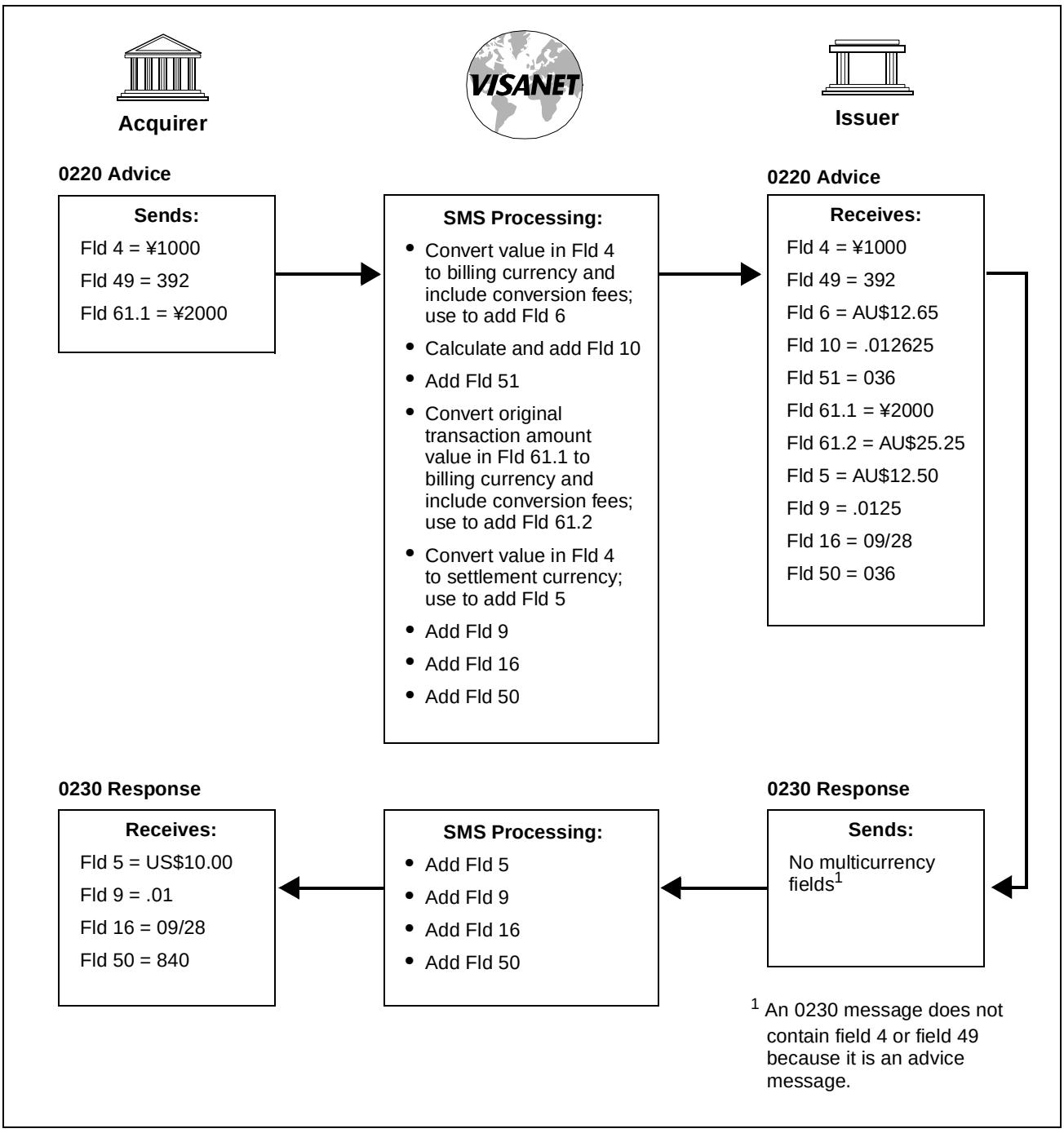
For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

Figure 5–6: Purchase Transaction



For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

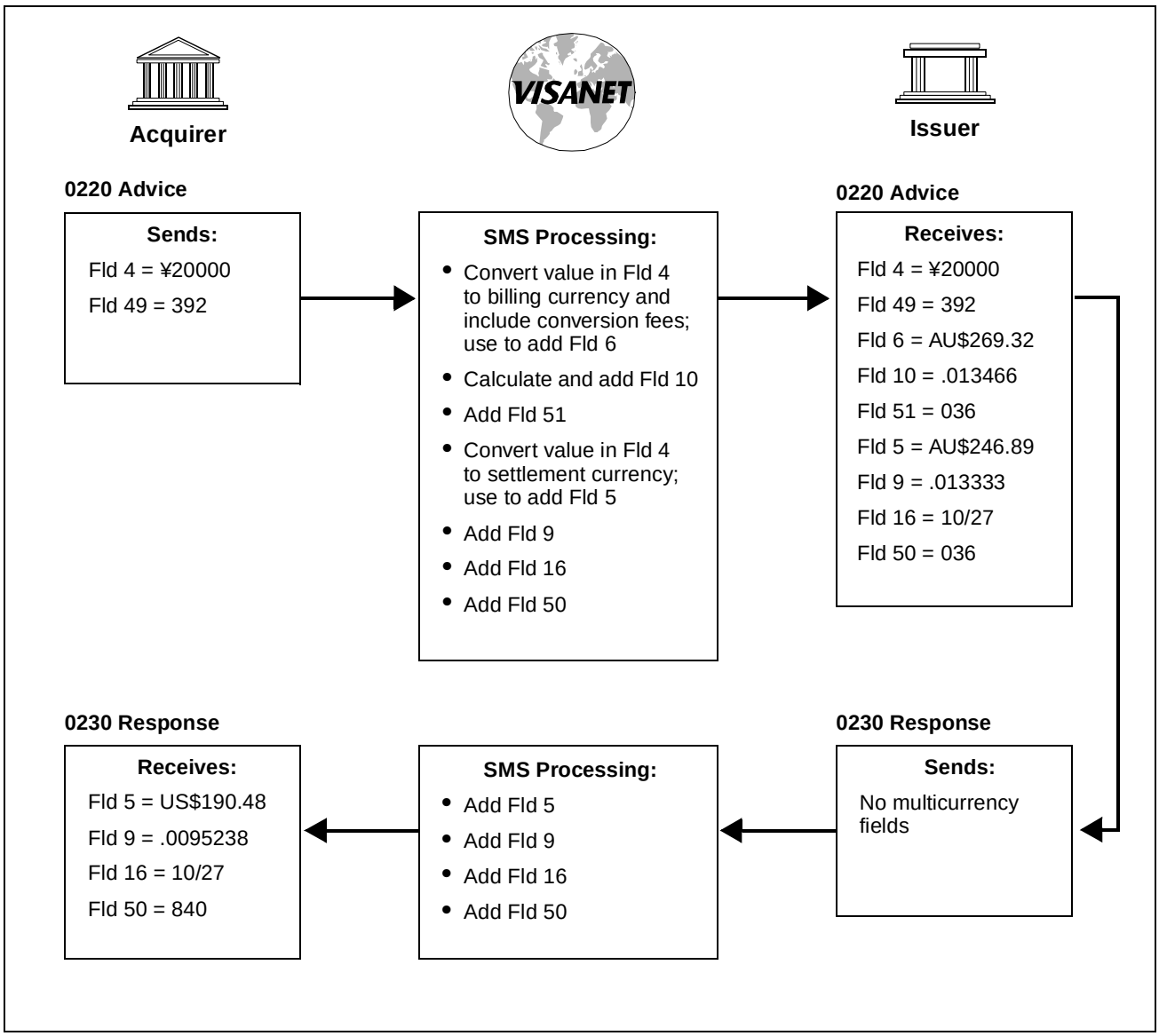
Figure 5–7: Adjustment



For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

Field 61.1 is used when the amount from the original transaction is different from the adjusted amount.

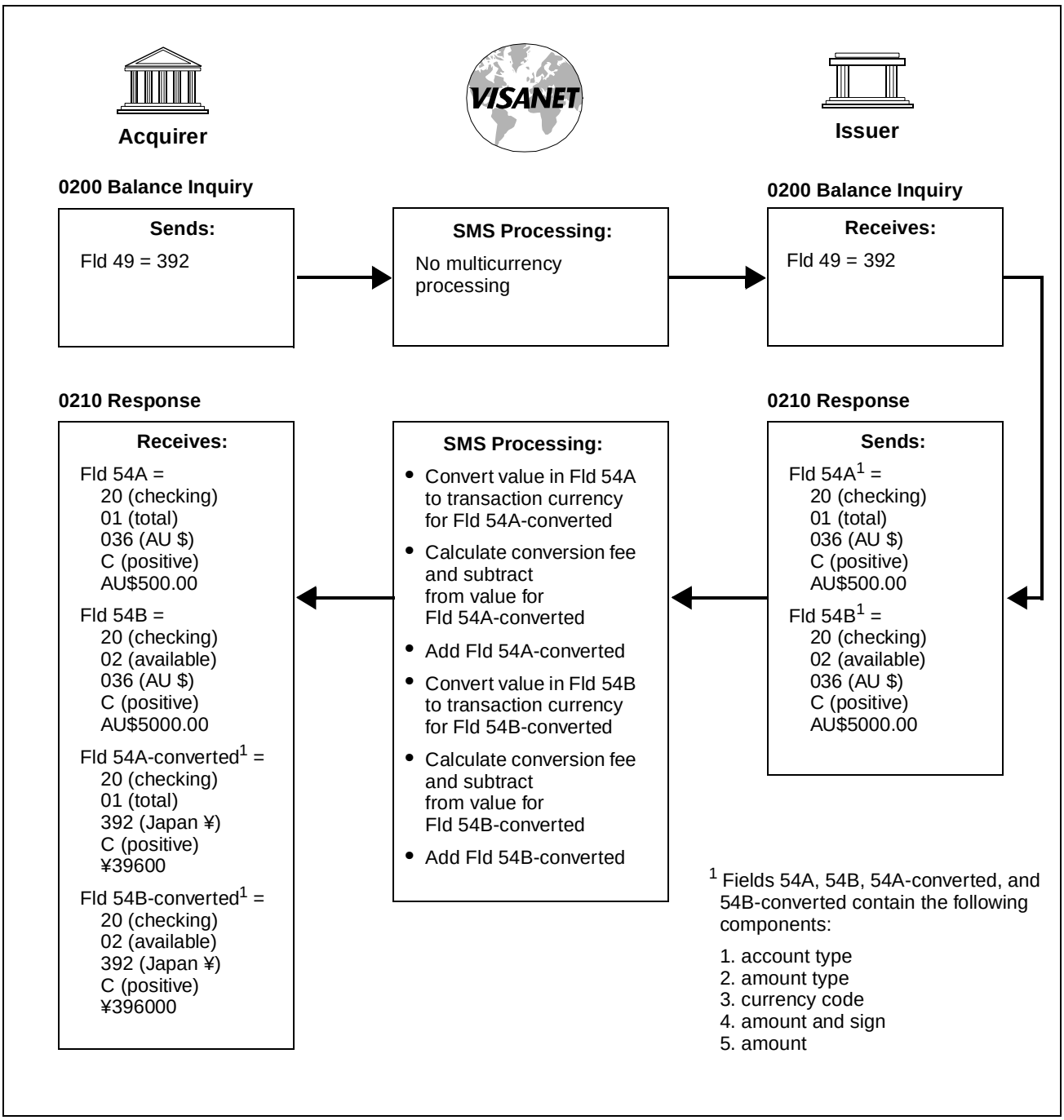
Figure 5–8: Representment



For this example, ¥105 = US$1.00 and AU$1.40 = US$1.00.

This example illustrates that the currency conversion rate can differ from the rate applied to the chargeback amount. (See the rates used in the chargeback example in Figure 5–11.)

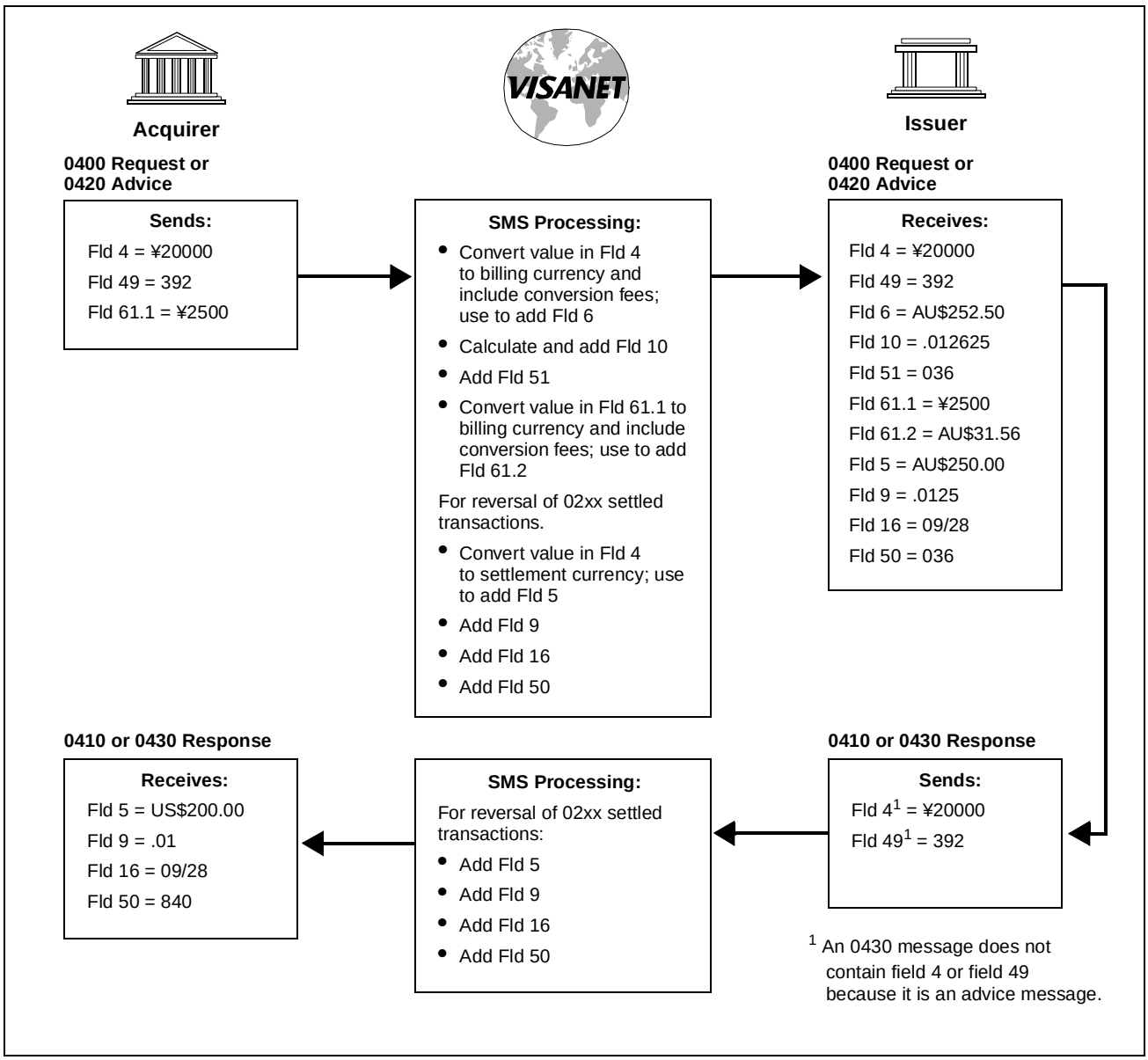
Figure 5–9: Balance Inquiry



For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

If field 54B is not provided, the acquirer center receives it zero-filled and does not receive field 54B-converted.

Figure 5–10: Reversal

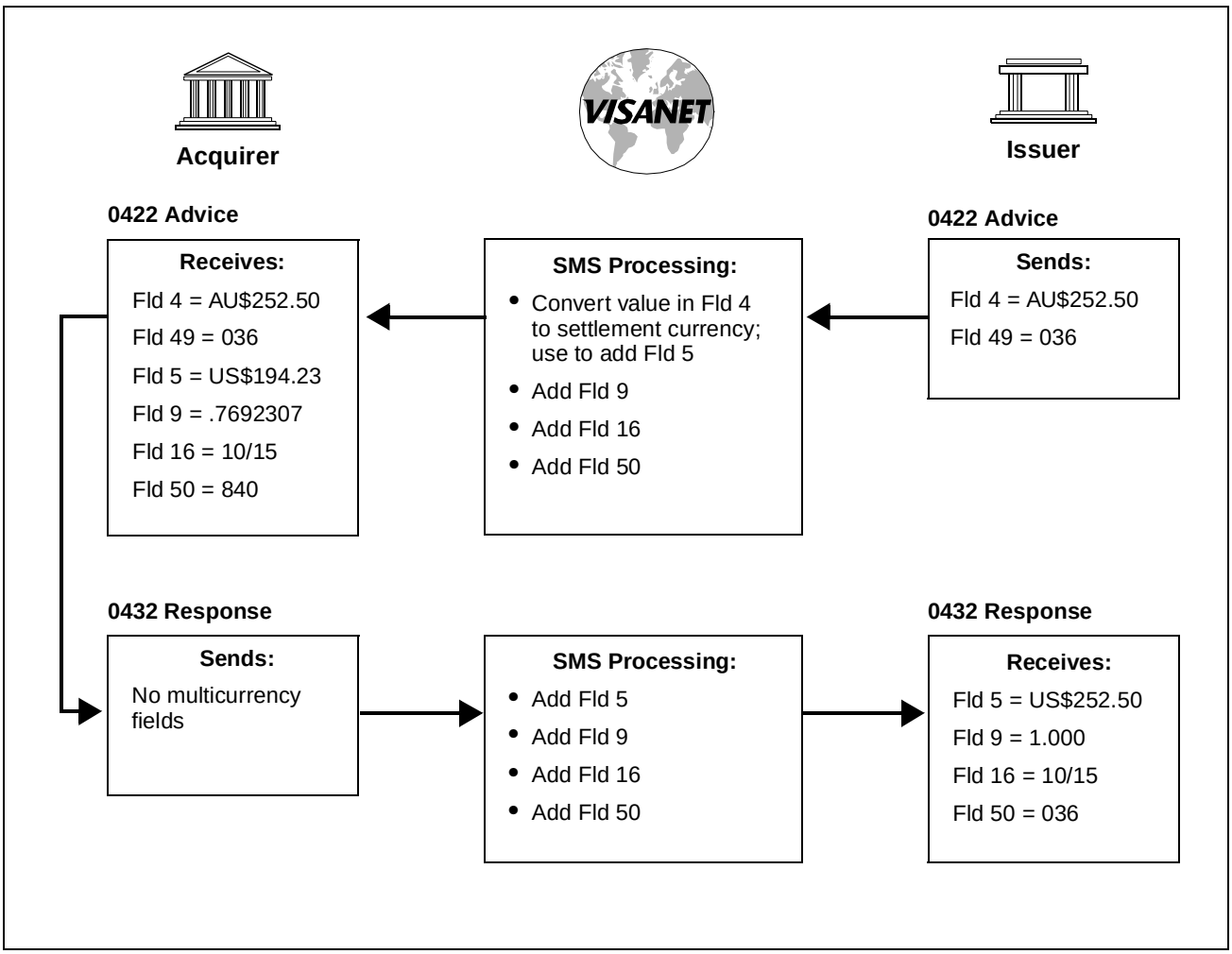


For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

Fields 61.1 and 61.2 in the request or advice message are used for the cashback amount of a purchase transaction, if any.

Under normal conditions, the acquirer sends an 0420 request to the issuer, and the issuer center responds with an 0430 message. Some acquirers continue to use 0400 requests and issuers need to be able to receive them. If the acquirer sends an 0400 request to the issuer, the issuer responds with an 0410 message. However, 0420 requests are recommended.

Figure 5–11: Chargeback—Full Amount

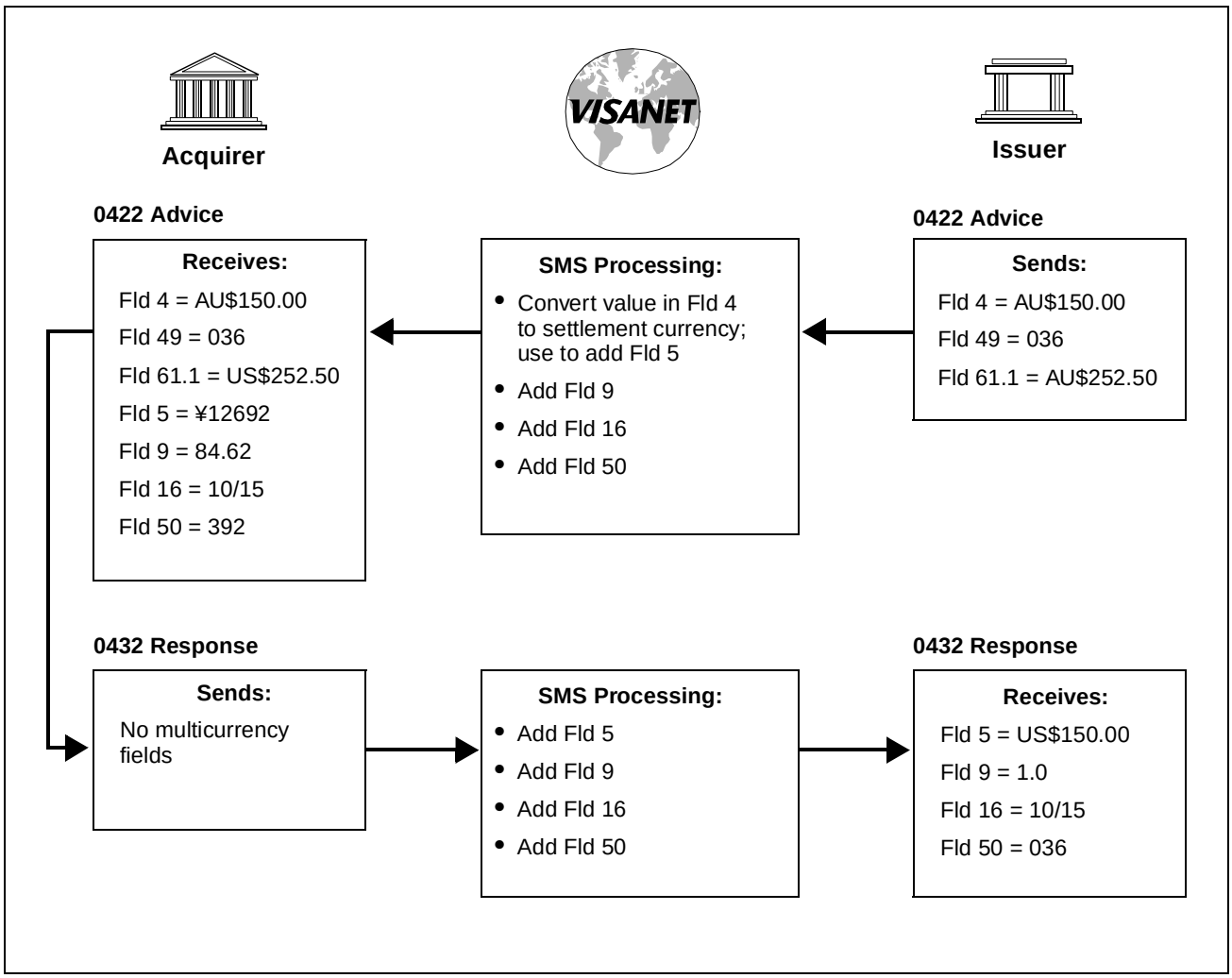


For this example, AU$1.30 = US$1.00.

The issuer uses the amount in Field 6—Amount, Cardholder Billing from the original transaction to fill Field 4—Amount, Transaction in the 0422 chargeback advice.

This example illustrates that the currency conversion rate can differ from the rate applied on the amount of the original sale. (See the rates used in the purchase transaction example in Figure 5–6.)

Figure 5–12: Chargeback—Partial Amount

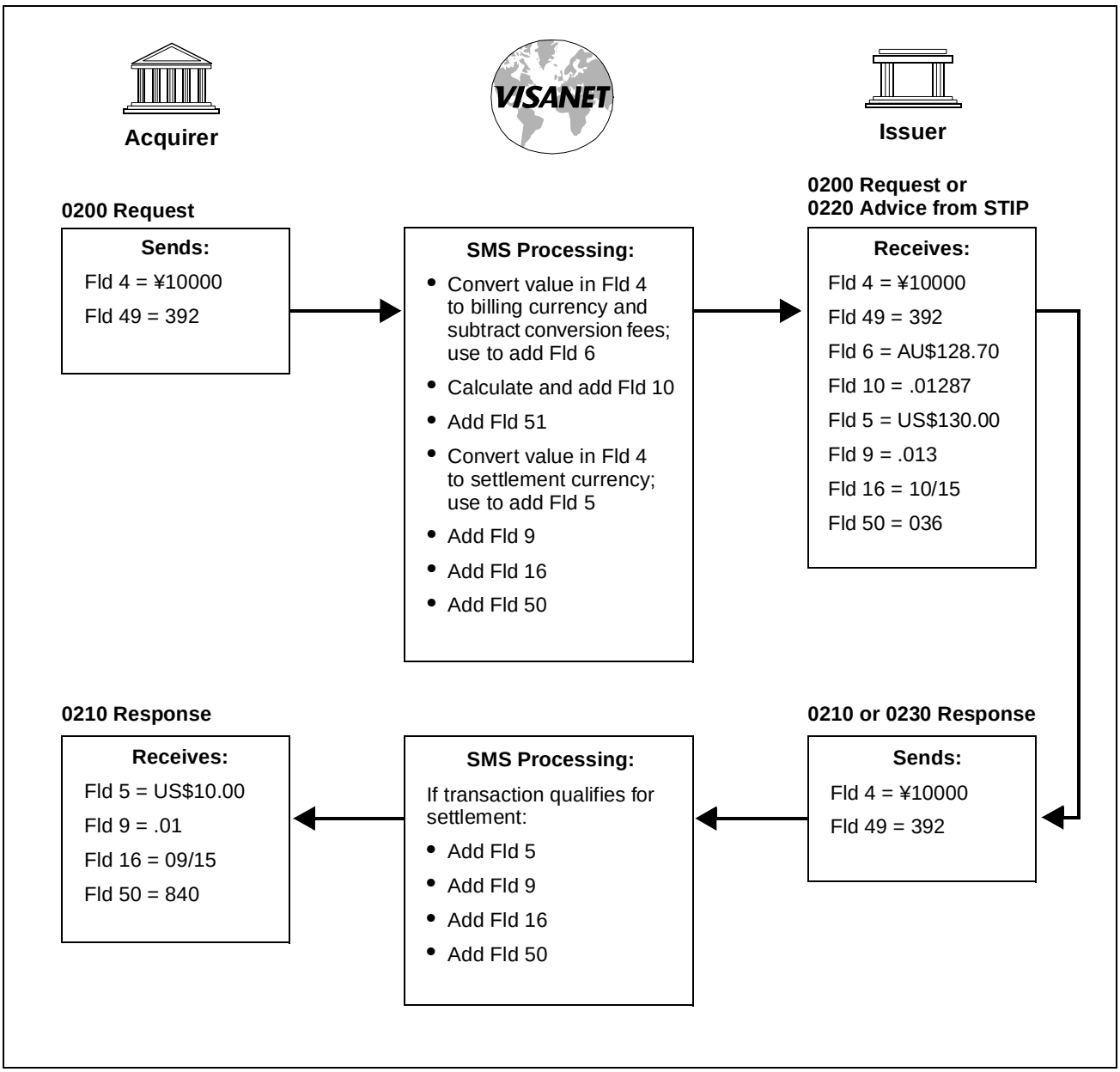


For this example, ¥110 = US$1.00 and AU$1.30 = US$1.00.

The issuer provides the chargeback amount in the cardholder billing currency. Field 61.1 is used to show the original transaction amount when it is different from the chargeback amount.

This example illustrates that the currency conversion rate can differ from the rate applied on the amount of the original sale.

Figure 5–13: Merchandise Credit



For this example, ¥110 = US$1.00 and AU$1.30 = US$1.00.

Stand-In and Card Verification Value Processing 6

This chapter includes discussions of:

- Stand-in processing, including the Positive Authorization Capacity Management (PACM) Service.
- Advice recovery for acquirers and issuers.
- The Card Verification Value (CVV and CVV2) services.

Stand-In Processing (STIP)

When an issuer is not available, SMS acts as a backup processor and authorizes or declines point-of-sale (POS) transactions on the issuer's behalf. This V.I.P. function is referred to as *stand-in processing*, or STIP.

All issuers specify the stand-in processing parameters to be used by SMS.

When an acquirer is not available to receive issuer-generated transactions such as chargebacks, SMS acts as a backup processor and accepts the transactions on the acquirer's behalf.

Conditions Requiring Stand-In Processing

STIP processes authorization requests (0100), financial requests (0200), reversal requests (0400), and reversal advices (0420) destined for an issuer under the following conditions:

- The line to the issuer is not available.
- The issuer is signed off.

- The issuer does not respond within a specified time limit.

  For Interlink, this limit is 10 seconds.

- The issuer is in recovery-only status.
- The issuer has been signed off by SMS due to 10 consecutive returned messages.
- The request is a reversal, the original transaction was approved by STIP, and the STIP advice of the original has not been recovered by the issuer.
- The request is for a preauthorization completion, the preauthorization was approved by STIP, and the issuer has not recovered advices.
- An issuer elects to use the Preauthorization Stand-In Service, defined later in this chapter.
- The issuer responds with Response Code 91—Destination Unavailable (an issuer option).

Issuer STIP Options

Issuers can specify the following STIP options:

- Setting transaction activity limits for card ranges and individual cardholders, such as:
  - Number of approved transactions for a particular account in one day (count)
  - Total value of approved transactions for this account in one day (amount)
- Using positive account controls through the Exception File for accounts that have VIP (very important person) status
- Using negative account controls through the Exception File for cards requiring declines
- Using modulus-10 check digit verification
- Requiring a valid card expiration date, either always or only if the expiration date is present
- Checking Personal Identification Numbers (PINs)
- Establishing PIN retry limits (if PIN checking is specified)
- Using Positive Authorization Capacity Management (PACM) Service
- Using Card Verification Value (CVV) Service
- Having STIP decline all transactions when the issuer is not available

STIP Authorization Processing

This section explains how STIP processes preauthorizations and financial transactions. Reversals are covered later in this chapter.

STIP uses up to four tests to check preauthorizations and financial transactions:

- Edit check
- Exception File check
- PIN check
- Activity check

Not all tests are done for all transactions:

- Balance inquiries are checked against the Exception File but are not tested for activity.
- PIN checking is performed only if specified by the issuer.

STIP approves financial requests unless it finds a negative condition. If the request passes all tests, STIP responds with an approval and creates an advice for later recovery by the issuer. STIP also updates the Activity File to reflect approvals made during the day.

If STIP finds a negative condition during any test, it assigns a decline response code to the request. This code is returned in Field 39—Response Code of the response, unless STIP finds a more serious decline condition in a subsequent test. If several response codes are assigned, STIP returns the code reflecting the most serious decline reason.

STIP rejects messages that contain consistency or syntax errors.

For balance inquiries, STIP assumes that requests are to be declined with Response Code 91—Destination Unavailable. If, however, the account is listed on the Exception File with a different decline code, STIP returns that code instead.

Edit Check

STIP edits the account number in Field 2—Primary Account Number for all requests. STIP also performs check-digit verification and checks the expiration date when specified by the user. STIP uses the date in Field 14—Date, Expiration or takes the date from the magnetic stripe data in Field 35—Track 2 Data.

In addition, STIP checks:

- The time limit in Subfield 63.2—Time (Preauth Time Limit) for preauthorization requests and preauthorization completion requests.
- The transaction amount (in Field 4—Amount, Transaction) in preauthorization completions.

The values in the account number, date, and time limit fields must meet syntax and consistency requirements. For example, if a request contains an incorrectly formatted expiration date or the date is not present, the request is rejected.

Account Number

The account number must have a valid modulus-10 check digit (if specified by the issuer).

The account number length must be valid for the range or ranges of numbers serviced by the issuer.

If the check digit or length is invalid, STIP assigns Response Code 14—Invalid Account Number, No Such Number as the decline response. STIP does not perform Exception File, PIN, or activity checks once the account number is determined to be invalid.

Expiration Date

STIP performs this edit if specified by the issuer.

Visa cards must contain standard data in track 2. If a card expiration date is present in the request, the date must not be expired. For a missing or expired date, STIP assigns Response Code 54—Expired Card or Expiration Date is Missing to the request. If the date is valid and there are no edit failures for other reasons, STIP assigns Response Code 00—Approved to the request.

To designate a nonexpiring card, issuers must use a value not greater than 20 years from the issue date or the value of 4912 in Field 35—Track 2 Data.

Time Limit and Amount in a Preauthorization Completion

The time limit for a preauthorization is two hours. If a preauthorization completion is submitted within two hours of the preauthorization request and the purchase amount is less than or equal to the preauthorized amount, STIP assigns Response Code 00—Approved to the request. STIP does not perform the Exception File and activity checks but does verify the PIN.

If the preauthorization time limit has expired, STIP responds with Response Code 91—Destination Unavailable.

If the purchase amount is greater than the preauthorized amount, STIP responds with Response Code 05—Do Not Honor.

Exception File Check

The Exception File contains account numbers that require special handling. Each Exception File record consists of an account number, a purge date, and an action code or cardholder spending limits or both.

Members can update the Exception File in batch or online mode. In batch mode, members prepare a tape containing the desired Exception File updates and send it to Visa. (See *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications* for detailed information.) SMS edits the updates for critical data such as account numbers and purge dates, then applies the updates to the Exception File.

Purchases

STIP checks purchases and preauthorizations against the Exception File to determine if an action code or cardholder spending limit is on file for the cardholder's account.

If no record is found—If the account is not on file, STIP performs the standard activity check.

If an action code is found—If STIP finds an action code for the account, it assigns that code to the request. The codes allowed in Exception File records for POS are:

05 = Do not honor.

11 = Approval for VIP (very important person)—A nonstandard activity check is needed. See the "Nonstandard Activity Checking" section of this chapter for more information.

If cardholder spending limits are found—STIP uses one of the following checks:

- If the Exception File contains limits but no action code, STIP uses the limits on file to check activity instead of the basic cardholder spending limits. STIP also checks the transaction limit and daily limits.
- If the Exception File contains limits and Action Code 11—Approval for VIP, STIP uses the limits on file for activity checking. STIP does not check the transaction limit and daily limits.
- If the file contains Action Code 11—Approval for VIP but no limits, STIP does not perform any cardholder activity checking.

Balance Inquiries

STIP checks balance inquiries against the Exception File to determine if a special decline code is on file.

- If the account is not on file, STIP assigns Response Code 91—Destination Unavailable.
- If the account is listed with a specific code, STIP assigns that code to the transaction.

STIP ignores records containing Action Code 11—Approval for VIP or activity limits, or both, for balance inquiries.

PIN Check

For users of the PIN Verification Service (PVS), STIP proceeds after the PIN is verified by SMS. If a PIN is invalid, STIP checks to determine if the incorrect-PIN limit has been exceeded.

For this test, STIP maintains a count of consecutive invalid PIN requests that it encounters on the current day for a given account number. STIP processing is based on the current PIN-incorrect count, as follows:

- The count (not including the current attempt) does not exceed the limit:
  - If the PIN is valid, STIP clears the count to zero.
  - If the PIN is invalid, STIP increases the count by one. It then compares the updated count to the limit. If the updated count now exceeds the limit, STIP assigns Response Code 75—Allowable Number of PIN Entry Tries Exceeded to the request.
- The count (not including the current attempt) exceeds the limit:
  - STIP assigns Response Code 75—Allowable Number of PIN Entry Tries Exceeded and does not update the count.
  - Once a count exceeds the limit, STIP continues to assign Response Code 75—Allowable Number of PIN Entry Tries Exceeded to all subsequent requests for the rest of the day. The cardholder is not able to complete any more transactions requiring a PIN for the rest of the day. The cardholder can retry the next day after STIP clears PIN counts at the end of the current day.

NOTE: *PIN Verification Service also can be used on a subscription basis for checking all PINs for an issuer, in addition to the STIP check.*

For more information on the use of PINs, refer to Chapter 7, Security.

Activity Check

This section describes the activity checking procedures that STIP performs when it receives a request.

IMPORTANT

This section does not apply to Interlink balance inquiries.

STIP checks cardholder activity using the contents of the Exception File and the following issuer-specified activity limits:

- Transaction limits
- Daily limits
- Cardholder spending limits

The activity check determines whether or not approval of the request causes the card usage to exceed these limits. If the activity is over the specified limits, STIP assigns Response Code 61—Exceeds Approval Amount Limit.

The activity check is based on activity accumulated daily in the Activity File. The accumulated totals are reset to zero every 24 hours. The Activity File contains only STIP approvals.

Standard Activity Checking

The standard activity check involves comparing:

- The amount of a request with the transaction limit.
- The request plus today's STIP approvals with the daily transaction count and amount limits.
- The request plus today's STIP approvals with the basic cardholder spending limits.

If the request exceeds the transaction limit, or approval of the request would cause total activity to exceed the daily or cardholder spending limits, STIP declines the request.

STIP performs the standard activity check on all requests it receives for processing unless the issuer has specified nonstandard activity checking on that account number, as explained in the following section, "Nonstandard Activity Checking."

Nonstandard Activity Checking

STIP can perform nonstandard activity checking on accounts that the issuer has listed in the Exception File as high-risk or low-risk accounts. If STIP finds an action code listed in the Exception File, it checks the limits in the Exception File instead of the standard activity limits. Refer to the "Exception File Check" section of this chapter for more information.

When Activity Is Not Checked

STIP does not perform the activity check in some cases because it is not needed to reach an authorization decision. The activity check is not done in the following cases:

- The request (for example, a credit adjustment transaction) results in a credit to the cardholder's account.
- The account is listed in the Exception File and the record contains Action Code 11—Approval for VIP, but there are no cardholder spending limits, indicating that activity checking is not required.
- STIP already assigned a decline response code during editing, the Exception File check, or the PIN check.

Excessive Activity

The amounts and counts must be less than or equal to all applicable limits. If activity is over the limit, the STIP response code indicates:

- The amount limit is exceeded (Response Code 61—Exceeds Approval Amount Limit).
- The count limit is exceeded (Response Code 65—Exceeds Withdrawal Frequency Limit).

If both conditions are true, STIP assigns Response Code 61—Exceeds Approval Amount Limit.

Assigning a Response Code

After editing the transaction and checking the Exception File, PIN, and activity, STIP assigns the appropriate response code to return in the response message.

- If only one code was assigned to a request, STIP returns that code in the response message.

  EXAMPLE

  If STIP assigns a Response Code 54—Expired Card or Expiration Date Is Missing during the edit, and finds no other decline conditions in subsequent tests, STIP returns the same Response Code 54 in the response message.

- If STIP assigns Response Code 00—Approved or Response Code 11—Approval for VIP and finds no decline conditions, STIP returns Response Code 00 in the response message. STIP never returns Response Code 11 in response messages to acquirers.

- If STIP assigns more than one decline code, STIP returns the most serious decline code.

The response codes are listed in the "Field 39" section of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*.

Updating the Activity File

When STIP approves a financial transaction, STIP updates the transaction totals in the cardholder's activity record as follows:

- Preauthorization requests

  STIP updates the Activity File.

- Financial, reversal, and Interlink POS cancellation requests:
  - STIP updates the count and amount totals for the approved request. STIP also updates the cardholder's grand totals.
  - For preauthorization completions, STIP also deletes the preauthorization segments.

Balance inquiries do not affect activity totals. Also, as explained earlier, PIN counts are updated as needed when the PIN is verified.

The accumulated activity totals either increase or decrease, depending on the value in Field 3—Processing Code in the request. Processing codes defined as having a debit value increase the totals, while credit processing codes decrease the totals. In reversals, debit processing codes decrease the totals, while credit processing codes increase the totals.

For a description of Field 3—Processing Code, refer to the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*.

Activity counts and amounts are never reduced to less than zero. If a credit adjustment exceeds the activity totals, STIP resets the activity record to zero.

Creating an Advice

When STIP responds to a preauthorization or a financial transaction, it always creates an advice for the issuer. Advice message types are:

- 0120 for an 0100 request.
- 0220 for an 0200 request.

A STIP advice contains all the data from the acquirer's request, except the PIN. The PIN field, Field 52—PIN Data, is zero-filled in the advice. (The zeros in field 52 notify the issuer that a PIN is present in the request.)

In addition to data from the acquirer's request, a STIP advice contains:

- STIP response code (in Field 39—Response Code).
- The reason STIP processed the request (in Subfield 63.4—STIP/Switch Reason Code).
- A value of 1 in the Advices-Created-By flag in the message header. (This value indicates STIP created the advice while standing in for the issuer.)
- Settlement flags in the message header of the advice. (STIP sets these flags as needed to indicate the settlement impact.) For more information, see the Message Structure and Header Field Specifications chapter of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*.

Advices remain on file until the issuer signs on to recovery status using an 0800 network management message.

Reversal Processing

Reversals cannot be declined. When STIP receives a reversal, it always approves the reversal and creates an advice for the issuer. STIP, however, edits the reversal for validity. STIP checks the reversal for proper syntax and consistency, and searches for the corresponding original transaction being reversed. If the original transaction is found, STIP updates the activity records and the reversal has financial impact. If the financial record is not found, the reversal has no financial impact so activity records are not updated. The issuer may still receive Response Code 00—Approved.

Updating the Activity File

When STIP approves a reversal, it updates the cardholder's activity record if the reversal has settlement impact. For example, POS counts and amounts are decreased for a valid reversal of a purchase transaction. The cardholder's grand totals are also decreased accordingly.

When a reversal has a credit effect on the cardholder's account, activity counts and amounts on file are never set to less than zero.

Creating an Advice

When STIP responds to a reversal, it creates an 0420 advice for the issuer to recover. The 0420 advice contains data from both the undeliverable reversal and the STIP response.

The Advices-Created-By flag of the 0420 message header contains a value of 1, indicating that STIP created the advice while standing in for the issuer. STIP also sets the settlement flags in the message header of the advice as needed to indicate the settlement impact. In addition, the 0420 advice also contains a reason code in Subfield 63.4—STIP/Switch Reason Code.

For more information, see the Message Structure and Header Field Specifications chapter of the appropriate *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*.

Positive Authorization Capacity Management (PACM) Service

Participation in PACM is optional for issuers.

PACM protects issuers against periods of excessive message volume by ensuring that their processing capacity is available for transactions with the greatest customer service and risk control implications.

When the volume of request messages exceeds the issuer's processing capacity, PACM routes a calculated number of low-risk transactions to STIP for the next minute. This diversion to STIP enables issuers to process higher-risk financial transactions, which reduces risk. PACM supports higher levels of customer service by reducing the frequency of inappropriate declines.

PACM also provides issuers with flexibility in scheduling processor upgrades.

PACM continually checks transaction volume every minute and adjusts the number of transactions routed to STIP so that the optimum number of messages can be processed by the issuer without exceeding the issuer's capacity.

PACM routes low-risk transactions to STIP, using a dynamic limit called the *Diversion Threshold*. STIP determines this limit by comparing transaction volume to issuer capacity.

Visa recommends that issuers review their activity checking parameters and default response codes before enrolling in PACM to avoid excessive STIP nonapprovals or high-risk exposure.

For more information on PACM, refer to *V.I.P. System Services*.

Acquirer Stand-In Processing

STIP provides stand-in processing for an acquirer when the acquirer is unable to receive issuer-generated messages including chargebacks, fee collection/ funds disbursement, and text messages. Stand-in processing occurs under the following conditions:

- The line to the acquirer is not active.
- The acquirer is signed off.
- The acquirer does not respond within a specified time limit.

SMS accepts the transaction on the acquirer's behalf and stores the transaction for the acquirer to receive through the advice recovery process. The advices contain information from the original issuer-generated request and include Field 63.4—STIP-Switch Reason Code.

Table 6–1 shows the advices the acquirer can receive.

Table 6–1: Advices for Acquirer

Issuer-Generated Request	STIP Advice to Acquirer
Chargeback (0422)	Chargeback (0422)
Text Message (0600)	Text Message Advice (0620)

Recovering Advices

An issuer or acquirer controls advice recovery by changing its network status maintained by SMS.

To start and stop the recovery of advices from SMS, acquirers and issuers use 0800 messages.

Table 6–2 shows the recommended values in the 0800 messages to sign on to and off of advice recovery status.

Table 6–2: Signing On and Off Advice Recovery Status

Station Type	Field 70 (Sign On)	Field 70 (Sign Off)
Common interface link V.I.P. message format	078	079

A station can be in normal signed-on mode, in advice-recovery mode, or in both modes concurrently.

- Normal status—If the station is signed on to normal status, it can receive and send real-time messages, but cannot receive advices from SMS.

- Recovery-only status—If the station is signed on to recovery status, SMS sends advices as they are stored. The station cannot initiate messages other than sign-on messages or the acknowledgment of advices.
- Normal and recovery status—If the station is signed on to both normal and recovery status, it can send and receive real-time messages and receive stored advices.

Timing of Recovery Status

Other than the system-induced advice recovery, there are no system requirements that dictate when or how often advices should be recovered. An acquirer or issuer can recover advices throughout the day or only during certain periods as it sees fit.

When an issuer designs its system, however, it should consider the impact of STIP authorization on advice recovery processing. STIP advices reflect authorization decisions that can affect the available funds in a cardholder's account. If the issuer restricts advice recovery to only certain periods, it may find that account balances are insufficient to cover the total value of issuer-approved and STIP-approved transactions.

Also, both issuers and acquirers should recover advices after a downtime condition, because advices from SMS can affect settlement accumulators as well as issuers' cardholder account balances.

Advice Recovery Flows

SMS keeps the following categories of advices until they are recovered by the issuer or acquirer:

- STIP processing advices
- SMS reversal advices
- Reconciliation totals advices
- Funds transfer totals messages

As previously stated, acquirers and issuers use 0800 messages to start and stop advice recovery from SMS. The flow that follows shows advice recovery by an issuer. A comparable flow is used for recovery by an acquirer.

IMPORTANT

The member should remain signed on during this process.

➤ **To Sign On to Recovery Status:**

1. To initiate advice recovery, the issuer sends an 0800 request, containing the applicable Network Management Information Code (078).

2. SMS replies with an 0810 response.

➤ **To Recover the Advices:**

1. SMS sends the highest priority advice on file.
2. The issuer replies with the appropriate acknowledgment.

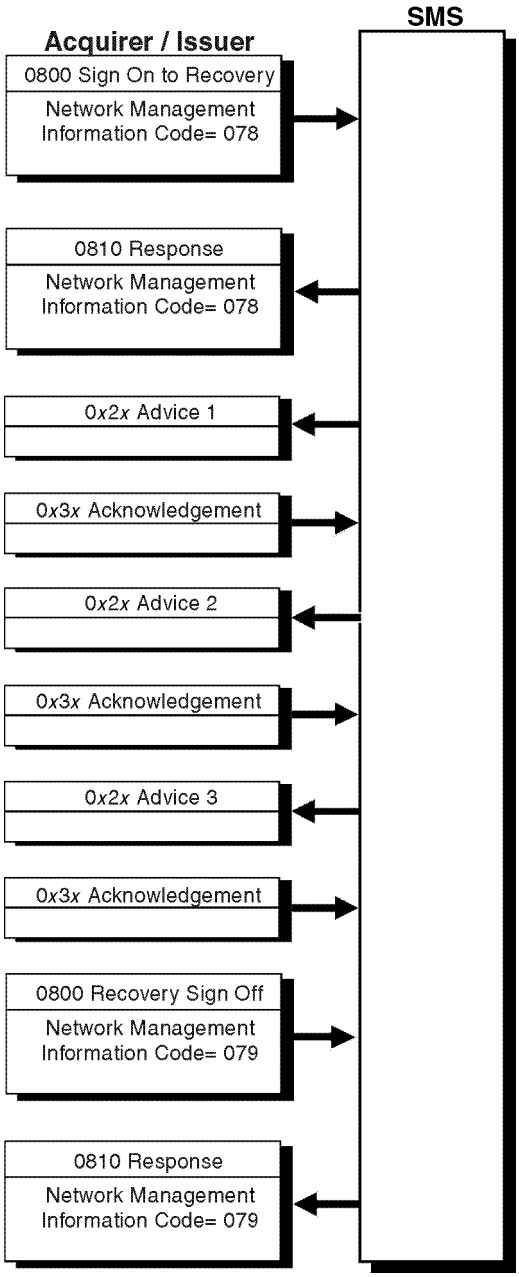
SMS continues to send advices, one at a time, in priority order. If the issuer does not acknowledge an advice, SMS resends the advice until acknowledgment occurs.

➤ **To Stop Advice Recovery:**

1. The issuer sends an 0800 message containing the applicable Network Management Information Code 079.
2. SMS replies with an 0810 response.

Figure 6–1 shows the message flow for advice recovery.

Figure 6–1: Advice Recovery Flow



Advice Flags in the Message Header

To provide additional information, Field 9—Message Status Flags in the message header contains three bits that are used as advice-related flags. SMS sets flags, and the issuer or acquirer can examine them during incoming message processing. For more information, see the Message Structure and Header Field Specifications chapter of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications.*

Preauthorization Stand-In Service for Issuers

The Preauthorization Stand-In Service is an optional service for Interlink that does not have the system capabilities to process preauthorization requests and preauthorization completions. When an issuer participates in this service, SMS stands in for all preauthorization request and completion transactions, and assigns STIP Reason Code 9032 to Subfield 63.4—STIP/Switch Reason Code of each transaction to indicate that it was processed by the service.

Preauthorization Limit

The preauthorization limit indicates the maximum amount that can be approved for preauthorization transactions processed by the Preauthorization Stand-in Service. The designated maximum amount for this limit is on a per-transaction basis, unlike the basic activity limits, which are cumulative throughout the day.

Interlink issuers that participate in the Preauthorization Stand-in Service are required to select a value for the preauthorization limit. In addition to the basic activity limits, all issuers must specify a preauthorization limit. The preauthorization limit can be a different value from those set for the basic activity limits.

Full and Partial Approvals

For a preauthorization request to receive a full approval when processed by this service, the request must pass all standard STIP editing tests described earlier in this chapter. In addition, the transaction request amount must not exceed the amount specified as the issuer's preauthorization limit.

SMS issues a partial approval if:

- The preauthorization request passes all STIP editing tests except the activity check.
- The full preauthorization amount requested exceeds any of the basic activity limits or the preauthorization limit set by the issuer, but a lesser, nonzero amount would be within the limits. This partial approval amount is the greatest amount possible without exceeding the limits.

Processing Preauthorization Transactions

STIP processes the following types of preauthorization transactions for issuers that participate in the Preauthorization Stand-In Service.

Preauthorization Requests

For preauthorization requests, STIP sends one of the following responses to the acquirer indicating the stand-in action taken:

- Full approval
- Decline

STIP does not create an 0120 preauthorization advice for the issuer.

Preauthorized Purchases

For preauthorization completion requests, STIP matches the request to a previously received preauthorization to determine whether the preauthorization completion request is within the two-hour time limit. If STIP finds a match and the time limit is not exceeded, it returns an 0210 approval response to the acquirer. If STIP does not find a match, it sends an 0210 decline response to the acquirer. Transactions over the two-hour time limit are not matched and are declined.

When STIP responds to the acquirer, it also sends an 0220 advice to the issuer indicating whether the response was a full or partial approval or a decline.

Reversals of Preauthorizations

For preauthorization reversals, STIP sends an 0410 response to the acquirer. STIP does not create an 0420 reversal advice for the issuer.

Reversals of Preauthorization Completions

For reversals of preauthorization completions, STIP sends an 0410 response to the acquirer. It also creates an 0420 reversal advice for the issuer.

If SMS receives a preauthorization completion reversal request that cannot be matched to a previously approved preauthorization completion message, the reversal advice for the issuer is flagged in the message header as having no settlement impact.

Card Verification Value (CVV) Service

The CVV Service is a risk control service that provides protection for issuers and acquirers against magnetic stripe counterfeit.

Participation in CVV is mandatory for all Interlink issuers. All Interlink cards must be encoded with CVVs.

NOTE: *The CVV Service provides support for Interlink transactions from proprietary cards, if the cards are encoded per Visa standards.*

Acquirers must ensure that the magnetic stripe data in financial requests is complete and unaltered.

The CVV is a unique check value calculated from the data encoded in the magnetic stripe using an algorithm established by Visa. The CVV is calculated using a secure cryptographic process and a key known only to the issuer and optionally to Visa. Because the CVV is not embossed or printed on the card, it can only be read from the magnetic stripe. Issuers utilizing CVV for magnetic stripe verification must place the CVV on track 2.

Both the acquirer and the issuer must be CVV participants for card verification to take place. The CVV is checked on all preauthorization and financial requests, using information supplied by the issuer and the acquirer.

A transaction is eligible for CVV checking when:

- The acquirer and the issuer are CVV participants (all acquirers are assumed to be participants).
- The transaction contains “90” or “02” in Field 22—Point of Service (POS) Entry Mode Code.
- The expiration date on the card is within the designated range for CVV checking.

When a transaction is processed, either Visa or the issuer’s host system calculates the CVV and compares it to the one encoded on the magnetic stripe. The CVV can fail CVV validation for any one of the following reasons:

- Fraudulent card
- Inaccurate reading or transmission of track 2
- Incorrect encoding of CVV, such as an incorrect position or wrong key

Issuer Processing Options

CVV checking is performed according to issuer-specified options as follows:

- Visa CVV validation
- Receiving CVV results

- CVV default response codes

Visa CVV Validation

Four Visa CVV validation options are available, depending on whether the issuer will be conducting the CVV tests, or if VisaNet will be conducting the CVV tests on the issuer's behalf.

The issuer processing options are:

ALL—VisaNet performs the CVV verification on all transactions and if the CVV validation fails, forwards the results to the issuer in the request message. The CVV verification results can be used with other risk management results to determine the appropriate response.

This option allows issuers to participate in the CVV Service without having to build a data encryption facility to conduct the tests.

ALL RESPOND—VisaNet performs the CVV verification on eligible transactions. If the CVV validation fails, Visa responds to the acquirer using the issuer's CVV default response code (or, a more severe response code determined by the stand-in processor, if applicable). VisaNet also creates an advice informing the issuer of the CVV results.

Since VisaNet responds to the acquirer with the issuer's CVV default response code, the issuer does not have the option to fully integrate this information with other risk control decisions.

(This option is not available in all regions. Contact a Visa representative for more information.)

STIP ONLY—The issuer performs CVV verification for all normal processing. VisaNet conducts CVV verification when the issuer's system is unavailable. VisaNet performs normal stand-in processing and conducts the CVV test. If the CVV validation fails, VisaNet responds to the acquirer with the issuer-provided CVV default response code, and indicates that the CVV validation failed in the financial advice to the issuer.

NONE—The issuer validates all CVVs. If the issuer is unavailable, STIP does not check the CVV. In this case, the CVV fails.

Receiving CVV Results

Whenever VisaNet performs CVV validation, VisaNet informs the issuer of the results of the validation by placing a value in either the original request message or in an advice message. The issuer has the choice to receive CVV results in either of the following fields:

- **Field 39—Response Code**

  If the issuer chooses to receive CVV results in Field 39—Response Code, the issuer receives a value of N6 when the CVV fails validation. If the CVV passes validation, the issuer receives no notification.

- **Field 44.5—CVV Results Code**

  If the issuer chooses to receive CVV results in Field 44.5—CVV Results Code, the issuer receives a value indicating either positive or negative notification of the CVV results:

  1 = the transaction failed CVV validation.

  2 = the transaction passed CVV validation.

  Blank (or not present) = the CVV was not tested; either the card was not encoded or a system error prevented CVV validation.

Participating issuers can also optionally send the CVV results of tests conducted by the issuer or VisaNet in field 44.5 of the response message. If the issuer returns field 44.5 in the response, the CVV results will be available to acquirers that have elected to receive this information.

CVV Default Response Codes

The issuer needs to inform VisaNet of the CVV default response code to be used when the CVV fails validation. The CVV default response code is used by Visa when it responds to the acquirer on the issuer's behalf. This applies to issuers when stand-in processing is required.

The issuer chooses one of the following default response codes:

00 = approve (not recommended for issuers using the ALL RESPOND option)

05 = decline

NOTE: *The response code in field 39 of advice messages may not be the same one that was sent to the acquirer. To preserve field 39 for the issuer, Visa recommends that issuers receive CVV results in field 44.5.*

Interlink CVV Transaction Processing

Table 6–3 summarizes the processing that occurs for each transaction type for

issuers participating in the Interlink CVV Service.

Table 6–3: Interlink CVV Transaction Processing Summary (1 of 5)

Transaction Type	For Participating Issuers		
	VisaNet Processing—Issuer Unavailable	**VisaNet Processing—Issuer Available**	**Issuer Processing**
Purchases (0200); purchases with cashback (0200); merchandise credits (0200); preauthorizations (0100); POS cancellations (0200)	VisaNet performs CVV validation for STIP ONLY, ALL, and ALL RESPOND options. If the CVV is invalid, VisaNet responds to the acquirer with the issuer's default response code. The advice to the issuer contains CVV results in field 44.5 or field 39 (results in field 39 are sent to the issuer only if the CVV fails and there is no higher failure detected by STIP).	VisaNet performs CVV validation for issuers that have selected the ALL or ALL RESPOND options. The message to the issuer contains CVV results in field 44.5 or field 39 (results in field 39 are sent to the issuer only if the CVV fails). ALL RESPOND option: If the CVV test fails, processing follows the description in the Issuer Unavailable column.	Two options apply: • Issuers that have selected the STIP ONLY option perform CVV validation (if the issuer is available). • Issuers that have selected the NONE option peform all CVV valiidation. If the issuer is unavailable, STIP does not check the CVV. In this case, the CVV fails. Available issuer performs standard authorization processing, taking into consideration the CVV results. At the issuers option, the issuer provides CVV results in field 44.5.
Preauthorizations (preauthorization stand-in service transactions only) (0100)	VisaNet performs CVV validation for STIP ONLY, ALL, and ALL RESPOND options. If the CVV is invalid, VisaNet responds to the acquirer with the issuer's default response code and creates an advice for the issuer.	VisaNet performs CVV validation for STIP ONLY, ALL, and ALL RESPOND options. If the CVV is invalid, VisaNet responds to the acquirer with the issuer's default response code. and creates an advice for the issuer.	Not applicable

Table 6–3: Interlink CVV Transaction Processing Summary (2 of 5)

Transaction Type	For Participating Issuers		
	VisaNet Processing—Issuer Unavailable	**VisaNet Processing—Issuer Available**	**Issuer Processing**
Balance inquiry (0200)	VisaNet does not perform CVV validation. VisaNet responds with a response code of 91.	VisaNet performs CVV validation for issuers that have selected the ALL or ALL RESPOND options. The message to the issuer contains CVV results in field 44.5 or field 39 (results in field 39 are sent to the issuer only if the CVV fails). ALL RESPOND option: If the CVV test fails, processing follows the description in the Issuer Unavailable column.	Issuers that have selected the STIP ONLY option or the NONE option perform CVV validation (if issuer is available). Issuer performs standard authorization, taking into consideration the CVV results provided by VisaNet. At the issuer's option, the issuer provides CVV results in field 44.5.
Reversals (0400, 0420)	VisaNet does not perform CVV validation. The advice does not contain CVV validation information.	VisaNet does not perform CVV validation since CVV was validated on the original transaction. POS Entry Mode of 90 is passed to the issuer.	The issuer receives 90 and, if it has the capability, it may perform CVV validation for its own monitoring purposes. Issuer may not deny the reversal based on the CVV validation results. The response to VisaNet should not include the CVV results in field 44.5.

Table 6–3: Interlink CVV Transaction Processing Summary (3 of 5)

Transaction Type	For Participating Issuers		
	VisaNet Processing—Issuer Unavailable	**VisaNet Processing—Issuer Available**	**Issuer Processing**
Store-and-forward purchases (0200)	No stand-in processing; acquirer receives response code 91 (destination unavailable).	VisaNet performs CVV validation for issuers that have selected the ALL and ALL RESPOND options. The message to the issuer contains CVV results in field 44.5 or field 39 (results in field 39 are sent to the issuer only if the CVV fails). ALL RESPOND option: If the CVV test fails, VisaNet responds to the acquirer with the issuer's default response code. The advice to the issuer contains CVV results in field 44.5 or field 39.	Issuers that have selected the STIP ONLY or the NONE option perform CVV validation (if issuer is available). Issuer performs standard authorization, taking into consideration the CVV results provided by VisaNet. At the issuer's option, the issuer provides CVV results in field 44.5.
Original resubmission (0200); store-and-forward resubmission (0200)	No stand-in processing; acquirer receives response code 91 (destination unavailable).	VisaNet does not perform CVV validation since CVV was validated on the original transaction. POS Entry Mode Code of 90 is passed to the issuer.	The issuer receives 90 and, if it has the capability, it may perform CVV validation for its own monitoring purposes. Issuer may not deny the reversal based on the CVV validation results. The response to VisaNet should not include the CVV results in field 44.5.

Table 6–3: Interlink CVV Transaction Processing Summary (4 of 5)

Transaction Type	For Participating Issuers		
	VisaNet Processing—Issuer Unavailable	**VisaNet Processing—Issuer Available**	**Issuer Processing**
Preauthorization completion (0200)	Completion received in less than two hours after preauthorization: VisaNet does not perform CVV validation. Approval is based upon normal completion processing. Completion received more than two hours after preauthorization: VisaNet responds with response code 91 (destination unavailable).	Completion received in less than two hours after preauthorization: VisaNet does not perform CVV validation. Approval is based upon normal completion processing. Completion received more than two hours after preauthorization: VisaNet performs CVV validation for issuers that have selected the ALL or ALL RESPOND options. The message to the issuer contains CVV results in field 44.5 or field 39 (results in field 39 are sent to the issuer only if the CVV fails). ALL RESPOND option: If the CVV test fails, VisaNet responds to the acquirer with the issuer's default response code. The advice to the issuer contains CVV results in field 44.5 or field 39.	Issuers that have selected the STIP ONLY option or the NONE option perform CVV validation (if issuer is available). Issuer performs standard authorization, taking into consideration the CVV results. At the issuer's option, the issuer provides CVV results in field 44.5.

Table 6–3: Interlink CVV Transaction Processing Summary (5 of 5)

Transaction Type	For Participating Issuers		
	VisaNet Processing—Issuer Unavailable	**VisaNet Processing—Issuer Available**	**Issuer Processing**
Preauthorization completion (preauthorization stand-in service transactions only) (0200)	Completion received less than two hours after preauth: VisaNet does not perform CVV validation. Approval is based upon normal completion processing. Completion received more than two hours after preauthorization: VisaNet responds with response code 05 (decline).	Completion received less than two hours after preauthorization: VisaNet does not perform CVV validation. Approval is based upon normal completion processing and the advice is sent to the issuer. The advice does not contain field 44.5 or field 39 with N6. Completion received more than two hours after preauthorization: VisaNet responds with response code 05 (decline).	Preauthorization completion advice received less than two hours after preauthorization: The issuer receives 90 and, if it has the capability, it may perform CVV validation for its own monitoring purposes. Completion received more than two hours after preauth: issuer will be notified by advice that the transaction was denied with an 05 (decline).

Issuer Requirements

The issuer who participates in the CVV Service is responsible for calculating and encoding the CVV on track 2 of the magnetic stripe and for providing Visa with the keys used for calculating the CVV.

NOTE: *Nonparticipating issuers will continue to receive a value of 02 on all transactions containing track 2.*

Calculating and Encoding the CVV

Participating issuers are required to encode the CVV on track 2 of the magnetic stripe according to the Visa-established standard for calculating the three-digit CVV and placing it on the magnetic stripe. The three-digit CVV can be generated by using a Visa Security Module (VSM), which is interfaced with the issuer's host system. If the issuer does not have a VSM, it can use its own program to generate the CVV, using the algorithm for computing the CVV.

Additional standards are included later in this section in "Placement of the CVV on Track 2" because current Visa CVV documentation, the "Card

Technology Standards" section of the *Card Technology Standards Manual*, defines standards for encoding track 2 only for 13-digit and 16-digit account numbers. With the introduction of the Plus CVV Service, track 2 data with encoded CVVs may contain account numbers with lengths from 12 to 19 digits.

Start Date for Service

The issuer must supply Visa with the expiration date of the first cards carrying the CVV. Any card with an earlier expiration date will not be tested for CVV. This allows VisaNet to process only those accounts that actually carry the CVV.

Placement of the CVV on Track 2

The issuer must identify the location of the CVV on track 2 of the magnetic stripe. Its location is given as the displacement from the end of the Service Code field. The placement of the CVV is used to determine that enough data is received in the magnetic stripe to contain the CVV and to locate the CVV for processing.

CVV Working Keys

The issuer must provide Visa with a pair of Data Encryption Standard (DES) keys to be used to generate and verify the CVV for track 2. The issuer sends these keys to Visa under the issuer's existing Zone Control Master Key (ZCMK). See Chapter 7, Security, for more information.

Visa recommends that the issuer not use the same verification keys for CVV as those used for PIN Verification Values (PVV) with the PIN Verification Service. If the common keys were compromised, it would affect both the issuer's PVVs and CVVs.

Issuer Verification

CVV verification is done by VisaNet when:

- The issuer is not available (STIP ONLY option).
- The issuer has selected the ALL and ALL RESPOND options.

CVV verifications is done by the issuer when the issuer has selected the STIP ONLY option or the NONE option and the issuer is available to process the transaction. Issuers performing their own CVV verification must follow these important procedures.

- Issuers must process all defined values for Field 22—POS Entry Mode Code.
- If the CVV is present and Field 22 contains a value of "90" (magnetic stripe read and entire contents are transmitted), CVV verification should be performed, depending on the issuer's parameters.

- If the CVV is valid:
  - The response should be based on the normal authorization criteria.
  - Field 44.5—CVV Results Code should contain the value of "2" (transaction passed CVV validation).
- If the CVV is invalid:
  - A Decline (05) response code should be generated.
  - Field 44.5—CVV Results Code should contain the value of "1" (transaction was checked for CVV and failed validation).

Acquirer Processing Options

Use of POS Entry Mode

Acquirers may submit a value of either "90" or "02" in Field 22—POS Entry Mode Code indicating that the acquirer has transmitted the complete, unaltered magnetic stripe. Visa strongly encourages using the value of "90". For Interlink transactions, the values of "90" and "02" are identical in meaning.

NOTE: *A value of 90 is required in the Asia-Pacific (AP) region.*

Receiving CVV Results

Acquirers can optionally receive the results of the CVV tests conducted by VisaNet or the issuer in Field 44.5—CVV Results Code. If the issuer does not provide the results in field 44.5, the results will not be available to the acquirer. Results will be provided to the participating acquirer when transactions have been processed in stand-in.

When requesting CVV results, the acquirer will receive a value as shown in Table 6–4.

Table 6–4: CVV Request Results Values

Value	Explanation
Blank or not present	Transaction was not CVV tested or the results were unavailable.
1	Transaction was checked for CVV and failed validation.
2	Transaction passed CVV validation.

Acquirers using this option can manage possible technical problems by monitoring the CVV Results Code in financial responses.

If the issuer does not provide the results in field 44.5 the results will not be available to the acquirer. Results will be provided to the acquirer when transactions are processed in stand-in.

Acquirer Requirements

Interlink acquirers must send the entire unaltered contents of the track data for all online magnetic-stripe-read transactions, indicate that the complete stripe has been sent, and be able to handle any resulting reject responses.

Acquirers must provide a positive indication that the complete, unaltered magnetic stripe is included in the authorization request.

- The value "90" in the first two positions of Field 22—Point of Service Entry Mode Code, is used to indicate the presence of the complete and unaltered magnetic stripe contents in the request.
- The entire, unaltered contents of track 2 must be present in Field 35 if Field 22 contains the value "90".

NOTE: *It is Visa's policy that CVV results will not be returned to the point of sale.*

CVV Certification

Issuers must be certified to participate in the Card Verification Value Service.

Issuers must certify that their cards are encoded correctly, that the appropriate keys have been established for STIP processing, and that they can perform CVV verification according to processing requirements. Depending on which processing option is selected by the issuer, the issuer certifies its capability to:

- Perform online validation of CVV.
- Accept either Response Code 82 (incorrect CVV) in Field 39—Response Code or Field 44.5—CVV Results Code.
- Accept POS Entry Mode Code value of "90" and the full magnetic stripe information in the authorization or financial request.
- Provide verification of CVV results in Field 44.5—CVV Results Code.

Once certification is accomplished, the issuer enters a monitoring period, where Visa monitors CVV values and system responses to ensure that the participant is supporting the requirements for CVV processing. Only after the monitoring process has verified that the participant supports these requirements does the issuer become a full participant of the service. For

details on the monitoring process, see the *Card Verification Value (CVV) Member Implementation Guide.*

Placement of the CVV

Track 2 has a maximum length of 40 characters and contains the following information:

- Start Sentinel
- Primary Account Number (PAN)
- Field Separator
- Country Code (only on valid track 2 with Primary Account Number beginning with 59)
- Expiration Date
- Service Code
- PIN Verification Value (optional)
- Discretionary Data
- End Sentinel
- LRC (Longitudinal Redundancy Check)

Start Sentinel, End Sentinel, and LRC are used by the magnetic stripe readers on terminals to ensure that they have correctly read the entire track. Track 2 data in field 35 must not include Start Sentinel, End Sentinel, and LRC. Excluding these three fields, 37 characters are available for encoding by the issuer. The Field Separator is included in track 2.

The CVV may be placed anywhere within the discretionary data. The length available for discretionary data will depend upon three other fields, the length of the Primary Account Number, the possible requirement to include the Country Code, and the option of encoding the PIN Verification Value.

Examples of track 2 data are shown in Table 6–5.

Table 6–5: Examples of Track 2 Data (1 of 2)

Field	Example 1	Example 2
Primary Account Number	16 digits	19 digits
Field Separator	1 character	1 character
Country Code (with 59)	not applicable	3 digits

Table 6–5: Examples of Track 2 Data (2 of 2)

Field	Example 1	Example 2
Expiration Date	4 digits	4 digits
Service Code	3 digits	3 digits
PIN Verification Value	5 digits	not applicable
Discretionary Data	8 digits available for placement of CVV	7 digits available for placement of CVV

Note that four digits will be available for the PVV if a CVV is encoded on a card with a PAN of 19 digits that begins with 59 (only cards with account numbers beginning with 59 are required to contain the country code on track 2). Four digits is sufficient for a Visa PVV, but may not be sufficient for other PVV algorithms.

CVV Displacement

To participate in the Interlink CVV Service, the issuer must inform Visa of the CVV location by indicating the number of positions it is displaced from the Service Code field (the number of positions between the last position of the Service Code field and the first position of the CVV). The first position of the displacement is referenced as position zero.

The following examples illustrate the placement of the CVV in the discretionary data.

CVV Displacement Example 1

The CVV has been encoded at a displacement of 8 from the Service Code. In this example, a PVV is also encoded on track 2. The CVV has been encoded in the fourth position of the remaining discretionary data, as shown in Table 6–6.

Table 6–6: CVV Displacement Example 1

Digit	PVV	PVV	PVV	PVV	PVV	DD	DD	DD	CVV	CVV	CVV	DD	DD
Displacement	0	1	2	3	4	5	6	7	8	9	10	11	12

CVV DISPLACEMENT EXAMPLE 2

The CVV has been loaded at a displacement of 0 from the Service Code. This example does not include a PVV encoded on track 2. The CVV is encoded in the first position of discretionary data, as shown in Table 6–7.

Table 6–7: CVV Displacement Example 2

Digit	CVV	CVV	CVV	DD	DD	DD	DD
Displacement	0	1	2	3	4	5	6

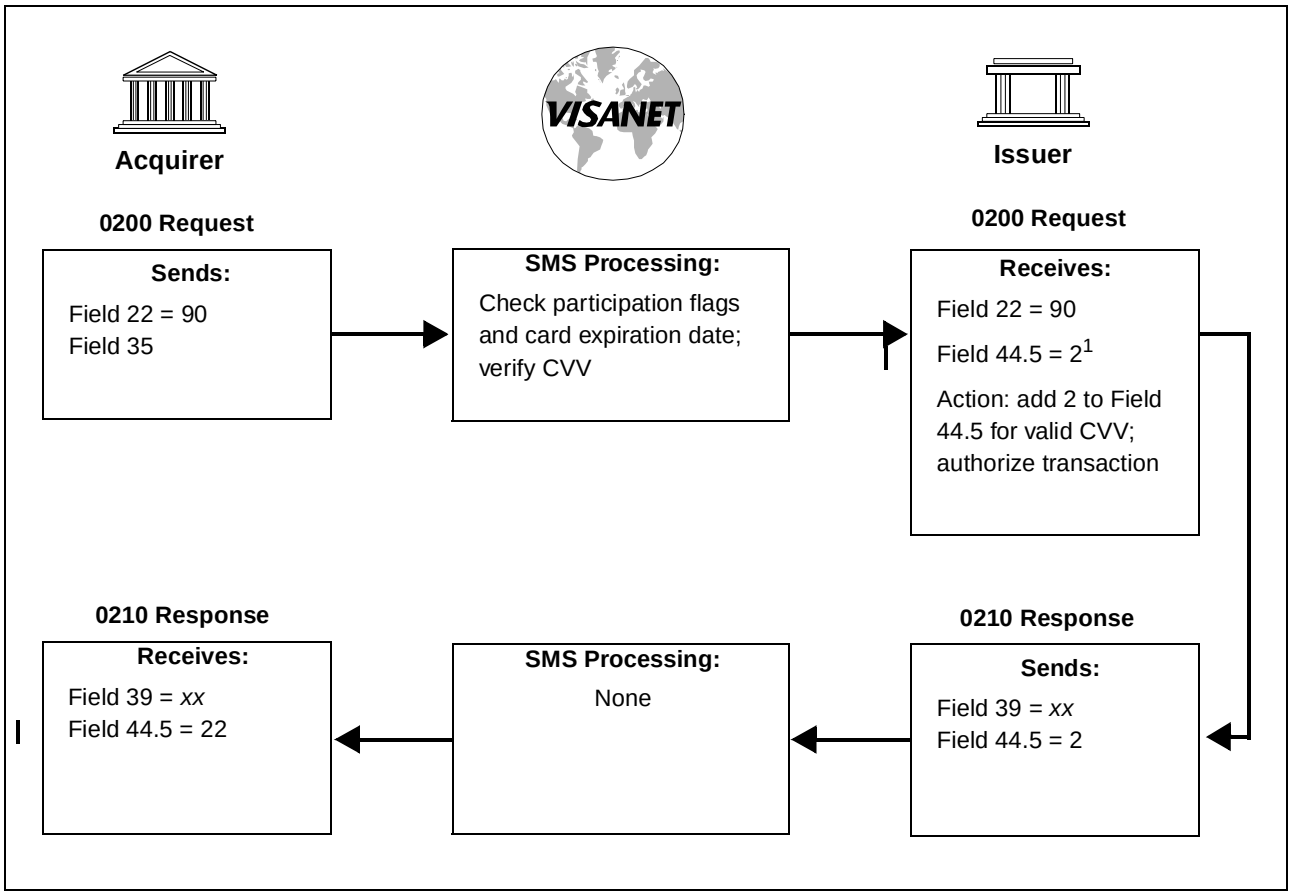
Refer to the "Card Technology Standards" section of the *Card Technology Standards Manual* for additional information on encoding the CVV.

CVV Flow

The flow shown in Figure 6–2 is an example of a transaction where:

- VisaNet validates the CVV.
- The CVV is valid.
- The issuer has selected field 44.5 to receive the CVV results and then incorporates the results in authorization decisions.
- The acquirer elects to receive the CVV results in field 44.5.

Figure 6–2: CVV Flow Example



[1] Only if the issuer has opted to receive the CVV results in field 44.5.
[2] Only if the acquirer is certified to receive the CVV Results Code in field 44.5.

Card Verification Value 2 (CVV2) Service

The Card Verification Value 2 Service is a card verification tool designed to reduce fraud losses when the card is not present. Issuers can imprint a 3-digit security number (the CVV2) on the back of Interlink cards, in accordance with applicable operating regulations.

Although a CVV2 value is never passed in Interlink transactions, Interlink cards can carry a CVV2 number for purposes of card activation, address changes, voice response unit (VRU) cardholder validation, and other bank customer service options to ensure that the cardholder has the “real” card in hand.

Security 7

This chapter contains an overview of security standards for Personal Identification Number (PIN)-based financial transaction interchange. These standards apply to all organizations acquiring or processing transactions containing PINs. Security considerations not directly related to financial transaction interchange are beyond the scope of this document.

The PIN discussion also contains:

- A description of the minimum acceptable standards for all branded services provided by any interchange network.
- An outline of the minimum acceptable standards for securing PINs and encryption keys.
- Procedures to help all participants in the retail electronic payment system establish assurances that cardholders' PINs are not compromised.

In addition to the Interlink bylaws and operating regulations, Interlink participants are also governed by the security standards and requirements in these documents:

- *Consolidated PIN Security Standards Requirements.*
- *Card Technology Standards Manual.*

This chapter reflects the information in *Consolidated PIN Security Standards Requirements.* The information provided in this chapter, however, cannot substitute for the specific rules in the manuals listed in this section. Contact your Visa representative for:

- Help getting copies of the security manuals and related information.
- Specific information about Interlink bylaws and operating regulations.

PIN Requirements for Interlink Participants

Personal Identification Numbers (PINs) are required for many Interlink transactions. For details, refer to the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications.*

PIN Security Overview

The PIN is a common convention used to verify the cardholder at the point of transaction. The value of the PIN as a means of verifying the identity of the cardholder depends exclusively on the secrecy of the PIN from the moment it is created, to the instant it is entered into the interchange system, and through the verification process used by the issuer.

Ensuring the confidentiality of the cardholder's PIN throughout the interchange cycle requires adherence to a set of recognized security standards to ensure the cryptographic protection of the cardholder's PIN. Such protection requires the implementation of specific controls to achieve the intended level of security by all participants. The standards described in this manual are the minimum acceptable standards for all branded services provided by any interchange network processing PIN-based transactions.

Failure to adhere to the specific controls and standards increases the risk of compromise to cardholder PINs. Such compromise would result in tangible dollar losses relating to the direct expenses required to correct and investigate fraudulent claims, as well as the erosion of consumer confidence in the payment system.

Card issuers expect that their customers' PINs will be protected throughout the interchange process. Acquirers depend on consumer confidence to facilitate the desired transaction volume. To ensure the value of interchange network branded services, this chapter outlines the minimum acceptable standards for securing PINs and encryption keys.

The successful management of payment system risks depends on the cooperation of all participants. There *must* be reasonable assurance that cardholders' PINs will not be compromised when used in the following devices belonging to other institutions or controlled by other networks and service providers:

- Automated teller machines (ATMs)
- Cash dispensers used at the point of sale (POS)

ANSI and ISO Standards

The ANSI and ISO standards referenced throughout this manual are:

- *Data Encryption Algorithm* ANSI X3.92-1981.
- *Personal Identification Number (PIN) Management and Security* ANSI X9.8-1982.
- *Personal Identification Number Management and Security* ISO 9564: 1991.
- *Modes of Data Encryption Algorithm Operation* ANSI X3.106-1983.
- *Financial Institution Key Management (Wholesale)* ANSI X9.17-1985.
- *Financial Institution Retail Message Authentication* ANSI X9.19-1986.
- *Financial Services Retail Key Management* ANSI X9.24-1992.

Security Responsibilities

Members are responsible for ensuring that they are in compliance with the requirements in *Consolidated PIN Security Standards Requirements*. It is their responsibility to make sure that their agents, card acceptors, vendors, and sponsored institutions are also in compliance.

Card Issuer Requirements

Each card issuer is responsible for ensuring the security and confidentiality of a PIN during generation, issuance, storage, and verification. The card issuer must be capable of performing PIN verification or having it performed through an agent.

Card issuers are responsible for advising cardholders not to disclose their PINs.

Acquirer Requirements

Each acquirer accepting PINs *must* be capable of accepting and translating encrypted PINs for interchange according to the requirements in this chapter. In addition, the acquirer *must* be able to perform key management as described.

Card Acceptor Requirements

Card acceptors *must* be capable of accepting and securely encrypting PINs of 4–6 digits in length in accordance with the requirements in this document. While not required, card acceptors are encouraged to support encrypting of PINs up to 12 digits in length.

Only the cardholder can enter the PIN. All other information relating to the transaction can be entered by either the cardholder or card acceptor. Card acceptors *must* never request cardholders to disclose their PINs.

PIN Management

To ensure the highest level of PIN security, controls *must* exist to minimize the risk of PIN compromise during entry, transmission, storage, and processing.

PIN Entry Requirements

All cardholder-entered PINs *must* be:

- Reversibly encrypted using the Data Encryption Standard (DES) algorithm either:
  - Within a Tamper-Resistant Security Module (TRSM) as specified in the "Tamper-Resistant Security Module" section of this chapter.
  - Within a minimum-acceptable PIN entry device, as specified in the "Tamper-Resistant Security Module" section.
- Encrypted and translated within a TRSM. TRSMs include PIN pads and hardware security modules.

Data Encryption Standard

Data Encryption Standard (DES) is a standard encryption technique used to protect critical information by enciphering data based on a 64-bit input key. The DES algorithm is described in ANSI X3.92-1981, *Data Encryption Algorithm*.

Members can choose to use either single-length DES or double-length DES (Triple DES) keys. Issuers and acquirers that choose to submit double-length DES keys must contact their Visa representatives.

Tamper-Resistant Security Module

Tamper-Resistant Security Modules (TRSMs) *must* be certified consistent with the guidelines in ISO 9564-1: 1991 (E) Section 6.3.1, "Physically Secure Device." A TRSM *must* have a negligible probability of being successfully penetrated to disclose all or part of any cryptographic key or PIN. A PIN entry device that complies with this definition can use Fixed Key or "Master Key/ Session Key" key management techniques. It can also use a unique key per transaction technique, as specified in Section 4.0 of ANSI X9.24-1992, *Financial Services Retail Key Management.*

A TRSM *must* be placed in service only if there are assurances that the equipment has not been subject to unauthorized modifications or tampering. Once TRSMs are placed in service, the following procedures and controls, at a minimum, *must* exist to detect or prevent unauthorized modification or tampering:

- The TRSM *must* be capable of detecting any fraudulent access or modification meant to disclose any cleartext PIN or key.
- If a TRSM can translate a PIN from one PIN block format to another, or if the TRSM verifies PINs, controls *must* be in place to prevent or detect repeated, unauthorized calls that could result in determining PINs.
- Controls *must* be in place to ensure that equipment is not reinstalled (when a suspicious alteration of a key in a TRSM is detected) until it has been inspected and a reasonable degree of assurance has been reached that the equipment has not been subject to unauthorized physical or functional modification.

Minimum-Acceptable PIN Entry Device

A minimum-acceptable PIN entry device *must* conform to the following specifications:

- The PIN *must* be encrypted using the DES algorithm within the device.
- The device *must* not permit disclosure of any PIN if penetration is successful, even with the knowledge of additional relevant data that is or has been accessible external to the device (for example, encrypted PINs as previously transmitted from the device). There *must* be no feasible way to determine the key used by the device to encrypt any PIN, given a knowledge of all data currently stored within the device, as well as all data transmitted to and from the device.
- The unauthorized determination of the secret data (PINs and keys) stored within the PIN entry device, or the placing of a “tap” within the device to record secret data, *must* result in physical damage to the device to the extent that the damage has a high probability of detection should the device be placed back in service. Furthermore, determining the data stored within the device *must* require specialized equipment and skills that are not generally available.
- A PIN entry device *must* use a unique key-per-transaction technique, as specified in Section 4.0 of ANSI X9.24-1992, *Financial Services Retail Key Management*.
- The data stored within a PIN entry device *must* not be able to be transferred into another such device.

- A minimum acceptable PIN entry device *must* be placed in service only if there is an assurance that the equipment has not been subject to unauthorized modifications or tampering.

PIN Transmission Requirements

For secure transmission of the PIN from the acquirer to the card issuer, the encrypted PIN block format described in this section *must* be used.

Encrypted PIN Block Format

PIN encryption in interchange between the point of PIN entry (ANSI PIN Block Format) and the point of PIN verification *must* be reversible so that the cleartext PIN block is recoverable at the point of verification.

The cleartext PIN block and the primary account number (PAN) must be exclusive-ORed (a mathematical operation, symbolized as XORed) together to form the standard ANSI PIN Block. This format is the PIN block format specified in ANSI Standard X9.8-1982, *Personal Identification Number (PIN) Management and Security* or ISO 9564-1:1991 (E), *Personal Identification Number Management and Security*.

PIN block format 1 (ANSI format 0) is required, except for members that use Triple DES keys. For these members, Visa recommends ISO PIN block format 3 where the keys are not changed.

The PIN block format specifies the number, position, and function of bits within a 64-bit block used as input to the DES algorithm operating in Electronic Code Book (ECB) mode (such as 64 bits in, 64 bits out). The 64-bit output of the DES algorithm is transmitted (or stored in the case of file protection) in its entirety.

Security may be enhanced if a double-length (112 bits plus parity) key is used for PIN encryption. The only acceptable method and sequence for double-length encryption is as follows.

Encrypting With the Double-Length Key

1. Encrypt the PIN block with the left half of the double-length key.
2. Decrypt this result with the right half of the double-length key.
3. Encrypt this result using the left half of the double-length key.

Encrypted PIN Block Rejection Criteria

Any Interchange Network Center having access to the cleartext PIN block *must* reject the encrypted PIN block if, during decryption, reformatting, re-encryption, or PIN verification, any of the following conditions are found:

- The Control field is not 0000 (binary).
- The PIN Length field value is less than 4 or greater than 12.
- A PIN digit has a value greater than 9.

When any of these conditions is met, a rejection *must* be transmitted to the sending node.

PIN Storage Requirements

PIN storage procedures *must* comply with Section 3.3 of ANSI Standard X9.8-1982, *Personal Identification Number (PIN) Management and Security* or ISO 9564-1:1991 (E), *Personal Identification Number Management and Security*. It is recommended that PINs not be stored. When necessary, they *must* be re-encrypted under a unique PIN encryption key not used for any other purpose. Access to stored, encrypted PINs *must* be strictly controlled. This control includes restricting both physical and logical access to the media used to store the encrypted PINs.

PIN-Based Store-and-Forward Transactions

Transactions can be stored and forwarded under certain conditions defined in various operating rules. When such conditions are present, any store-and-forward transaction PIN *must* be stored in encrypted form. When the key under which the PIN was originally encrypted is not available, the following procedure must be used: the PIN must be translated from the Zone Working Key used in transmission to a “local” PIN Encryption Key within a security module and then stored and encrypted only as long as it is needed to obtain authorization.

Once transmission is possible, the PIN *must* be translated from the local PIN Encryption Key into the appropriate Working Key for transmission to the next host.

PIN Verification Requirements

The card issuer is responsible for verifying the cardholder’s PIN. The issuer or its agent can perform this function on either a permanent or stand-in arrangement. Each card issuer *must* use its own unique keys for stand-in verification. These keys are to be maintained using the same principles for safekeeping as for all other encryption keys used to provide PIN security.

PIN Verification Keys *must* be uniquely created and *must* not be related to any other encryption key except by chance. Compromise of a PIN Verification Key could result in the disclosure of all cardholder PINs using that particular key. Such a compromise would require reissuing of all cards with PINs derived from the compromised key.

PIN Verification Service (PVS)

PVS is an SMS service that provides verification of personal identification numbers (PINs) used for Interlink transactions. Card issuers are responsible for verifying their cardholders' PINs.

At the issuer's option, SMS can verify PINs on behalf of the issuer, at all times or only when the issuer is unavailable. When SMS verifies PINs, it intercepts all requests, verifies the PINs, and passes the requests to the issuers or the SMS stand-in processor (STIP), as appropriate, for processing.

Issuers can use either of the following options for encrypting PINs:

- The encrypted PIN for a given card can be encoded on that card's magnetic stripe.
- The encrypted PIN for each account can be stored in Visa's database.

In either case, the issuer's PIN Verification Key (the key used to derive the PINs) must be sent to Visa. This is done by encrypting the PIN Verification Key using the Zone Control Master Key (ZCMK) that is established between Visa and the issuer as described in "Key Management and Security" later in this chapter.

Visa currently offers these methods for calculating the encrypted PIN:

- Visa PIN Verification Value (PVV)
- IBM PIN Offset
- Atalla Technovations Encryption systems

For more information, refer to:

- "PIN Check" in Chapter 6, Stand-In and Card Verification Value Processing.
- The *Card Technology Standards Manual* for information on computing and placement of the PVV.
- The *IBM 3624 Computer Transaction Facility Programmer's Reference and Component Descriptions* manual for information about the IBM PIN Offset method. Contact IBM for a copy of this manual.

Key Management and Security

To ensure the highest level of key security, controls *must* exist to minimize the risk of keys being compromised during creation, transmission, loading, administration, and destruction. This section outlines the minimum acceptable standards for providing adequate key security.

Key Creation Requirements

Keys must be created using a random or pseudo-random process as described in ANSI X9.17-1985, *Financial Institution Key Management (Wholesale)*. Keys must be generated by using statistical randomness such that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys.

Where two organizations share a key to encrypt PINs communicated between them, that key *must* be unique to those two organizations and *must* not be given to any other organization. This technique of using unique keys for communication between organizations is referred to as *zone encryption* and is described in the "Zone Encryption" section of this chapter. Inter- and intra-zone encryption is required.

Zone Encryption

VisaNet uses the *zone encryption* scheme to ensure PIN secrecy as requests pass from acquirers to VisaNet and to issuers.

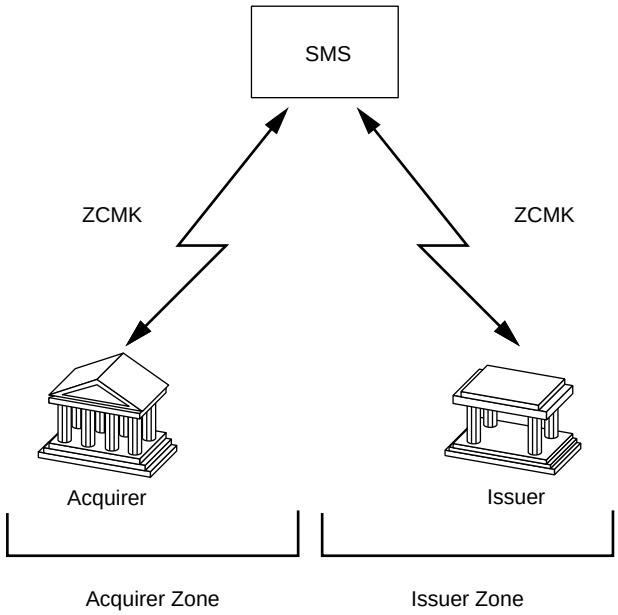
PIN processing in a DES-based zone encryption scheme is characterized by two zones: an acquirer zone and an issuer zone. SMS is a participant in each of these zones and functions as a cryptographic intermediary.

A zone begins at a TRSM device that encrypts the PIN and ends when the encrypted PIN is decrypted at a TRSM using the same cryptographic key that originally encrypted the PIN. The security of zone encryption, and the ability to change keys used within a zone without affecting other zones, is dependent upon using a unique Zone Control Master Key (ZCMK) for each zone.

The ZCMKs are used to encrypt Working Keys. All PIN Encryption Keys conveyed between the two organizations *must* be encrypted under these ZCMKs.

Figure 7–1 illustrates an example of zone encryption.

Figure 7–1: Zone Encryption



The acquirer's security zone begins at the point of PIN entry and encryption and ends at the next point of PIN decryption. The issuer's security zone begins at the point of PIN encryption where the Issuer's Working Key (IWK) is first used and ends at the issuer's processor. Issuers are strongly encouraged to process PINs within the confines of a hardware security module. There may be several intermediate security zones between these two points where PIN translations are performed in Physically Secure Devices (PSDs). At no time in the zone encryption process are PINs to be translated in software.

PINs must be encrypted from point of entry to the acquirer. Keys reserved for local use, however, can be used to encrypt PINs in on-us and interchange transactions from point of entry to the acquirer. Before sending the transaction to SMS, the acquirer center must encrypt the PIN using an Acquirer Working Key (AWK).

When SMS receives a transaction, SMS determines where the PIN is to be verified and whether the request is destined for the issuer or a stand-in processor for authorization. If the request is destined for the issuer's center, SMS acts as an intermediary by performing PIN translation. Before the PIN is sent to the issuer's center, SMS must encrypt the PIN using the applicable IWK.

The AWK *must* only be known by the acquirer and SMS. The IWK *must* only be known by the issuer and SMS.

Key Uniqueness

Encryption keys *must* only be used for the purpose they were intended; for example, Key Encryption Keys (KEKs) are not to be used as Working Keys. This precaution is necessary to limit the magnitude of exposure should any key or keys be compromised. Using keys only as they were intended to be used also significantly strengthens the security of the underlying system. Keys should never be shared or substituted in a processor's production and test systems.

Any key used to encrypt a PIN in a minimum acceptable PIN entry device *must* be known only in that device and in security modules at the minimum number of facilities consistent with effective system operations.

Weak Keys

Weak keys *must* not be purposely generated. Weak keys are defined as those keys that create the same results during both encryption and decryption.

Key Component Generation

When the physical key components are generated, there *must* be at least two components, each 16 characters in length. The encryption key is then created by a process of XORing the separate 16-character components together to create a unique encryption key. The XORing process is to be managed inside a TRSM.

Two or more components *must* still be created for devices requiring manual entry of a single encryption key. The components are parts of the single key (for example, left eight digits and right eight digits).

Transmission Requirements

Because the DES is a symmetrical encryption algorithm, keys *must* be shared between communication nodes. Encryption keys can be initialized between nodes by forwarding the hardcopy key components to the opposite node using different communication mediums, for example:

- Regular mail and overnight mail services.
- A cryptogram of the encryption key.
- A cryptographic entry pad under a key shared between the two nodes.

An encryption key, typically a KEK, *must* be transferred by physically forwarding the separate hardcopy components of the key using different communication channels or transmitting them in ciphertext form.

Dynamic exchange of the ciphertext form of Working Keys used for PIN encryption reduces the risk associated with manually maintaining Working Keys at many different locations. The Working Keys *must* be changed at random to reduce the window of exposure associated with compromising the keys.

Dynamic Key Exchange Service

Visa offers a Dynamic Key Exchange Service. The Dynamic Key Exchange Service offers members the following two alternatives for key conveyance using 0800 and 0810 network management messages:

- The member sends an administrative request to SMS at random intervals for a new acquirer or a new issuer working key. Upon receipt of the request, SMS generates the appropriate working key and sends it online to the member.
- The member designates SMS to:
  - Generate automatically new acquirer or new issuer working keys at a set time during the day.
  - Send new keys before sending an authorization request to the issuer.

To ensure that the participant and SMS are using the same keys, the participant must acknowledge successful receipt of a new key.

For details about this service, refer to the "Dynamic Key Exchange" section in Chapter 4, Message Types and Flows.

Hardcopy Form

Hardcopy key parts are the separate parts of a cleartext key that have been created for transport to another endpoint in a symmetrical cryptographic system. Typically, hardcopy key parts exist for KEKs, that is, keys used to encrypt Working Keys for transport across some communication channel. Until such keys can be protected by encryption or by inclusion in a PSD, the separate parts *must* be managed under the strict principles of dual control and split knowledge.

Dual control means that each hardcopy key part *must* be controlled by the single individual designated as the key custodian for the specific key part. *Split knowledge* means that separate individuals can have custodial control of key components, but each component must not convey knowledge of the resulting cryptographic key.

Ciphertext Form

Once the initial keys have been established, encryption keys can be transmitted in ciphertext form or within a PSD.

Key Loading Requirements

The DES algorithm is reversible. The cryptographic keys must be shared between endpoints to decrypt the encrypted PINs and perform PIN translation. Because the same encryption key exists in two different locations and the security of the cryptographic process depends on the secrecy of the encryption key, the loading of the keys into TRSMs and into the host processing system *must* be managed using highly controlled and secure procedures.

When encryption keys are established, a key has to be communicated from the point of origin to the next logical node on the communication link. This communication is accomplished through the transfer of hardcopy key components. Until the key components have been cryptographically secured, they *must* be maintained using the principles of dual control and split knowledge.

Host Key Loading Practices

The following practices apply to host key loading:

- The host processing environment controls the Master File Key, KEKs, and Working Keys. All keys managed at the processing level *must* be stored encrypted under the host Master File Key or maintained in the hardware security module.
- When loading the Master File Key and any KEK from the individual key components, centers *must* use dual control and split knowledge. Procedures *must* be established that prohibit any one individual from having access to all components of a single encryption key. Individuals entrusted with a key component *must* ensure that no person (not similarly entrusted with that component) can observe or otherwise ascertain the component before, during, and after key loading.
- Any EPROMS and EEPROMS used to load encryption keys *must* be maintained using the same controls used to maintain the security of the hardcopy key parts.
- Any hardware used in the key loading function *must* be controlled and maintained in a secure environment. Use of the equipment should be monitored and a log of all key loading activities maintained for audit purposes. All cable attachments *must* be examined before each application to ensure that there has been no tampering.
- Working Keys are typically created by the hardware security module. Working Keys *must* never exist outside a TRSM or a hardware security module in any form other than a cryptogram.

- All high-level key loading procedures *must* be created to be consistent with the key loading requirements of the hardware processing software and the unique security features of the hardware security module used for hardware security.

Key Loading at the PIN Entry Device

The following practices apply to key loading at the PIN entry device.

- Encryption keys are loaded either as two or more components or injected directly into the TRSM using a secure transfer device. When keys are loaded manually, the principles of dual control and split knowledge *must* govern the process. Procedures *must* be established that prohibit any one individual from having access to all components of a single encryption key. Individuals entrusted with a key component *must* ensure that no person (not similarly entrusted with that component) can observe or otherwise ascertain the component before, during, and after key loading.
- When keys are loaded to a PIN pad by using a secure transfer device, controls *must* be established that prohibit unauthorized use or substitution of equipment. The key *must* be erased from the transfer device after transfer to a terminal or PIN entry device. The key transfer device *must* be loaded under dual control to prevent unauthorized modification or tampering.
- Many vendors provide software applications for loading encryption keys into PIN entry devices. This software usually runs on a personal computer and, in all situations, the key that is injected into the PIN entry device is resident in the random access memory of the microprocessor. The personal computer is not a PSD. In all situations, this process *must* be managed so that the key loading function is consistent with the standards identified in *Consolidated PIN Security Standards Requirements* and that the intended security of the keys to be injected is maintained to ensure that the keys are not compromised.
- Any hardware used in the key loading function *must* be controlled and maintained in a secure environment. Use of the equipment should be monitored and a log of all key loading activities maintained for audit purposes. All cable attachments *must* be examined before each application to ensure that there has been no tampering with the equipment.

Key Storage and Distribution

The following practices apply to key storage and distribution.

- Cleartext keys, that is, keys that are either not encrypted or not maintained under the principles of dual control and split knowledge, *must* exist only inside a device that is physically secure.

- Cryptographic keys *must* be hierarchically stored if they are stored in their ciphertext form or communicated to a device to facilitate an electronic key change function. A hierarchy of encryption keys includes Master File Keys, KEKs, and Working Keys.
- The sharing of keys within a network works well when the network is small, but becomes increasingly cumbersome in large systems. Regardless of the situation, when keys are shared between and within encryption zones, procedures *must* exist that ensure the security of the key components during the distribution process. For example, dual control and split knowledge must be used, assuring that no single person has full knowledge of the encryption keys.

  When encryption keys are established, a key has to be communicated from the point of origin to the next logical node on the communication link. By transferring hardcopy key components. Until the key components have been cryptographically secured, they *must* be maintained following key administration requirements.

Key Administration Requirements

Key administration practices require protecting the key or keys from disclosure or substitution, or both. Procedures to restrict the use of encryption keys and methods to limit the effects of key compromise also are important. Key administration also must provide for key replacement and destruction standards.

Protection Against Key Disclosure

Any cryptographic key *must* exist only:

- In an encrypted form.
- In a TRSM or a minimum acceptable PIN entry device.
- In at least two components, in which every bit of the key depends, independently, on every other bit of the key. (That is, the key is formed by XORing the two components together.)

  Each key component *must* be in the physical possession of only one person or group of persons considered trustworthy. The person or group of persons *must* be instructed to keep secret the component entrusted to them.

  If the component is not in human-readable form (for example, in a PROM module), it *must* be in the physical possession of only one person or group of persons and for the minimum practical time.

If the component is in human-readable form (for example, printed, as within a secure mailer), it *must* be known to only one person (or alternate) and only for the duration of time required for this person to enter the key component into a TRSM or a minimum acceptable PIN entry device.

A single component *must* never be in the physical possession of a person or group of persons when any one such person is or ever has been similarly entrusted with any other component of this key.

Protection Against Key Substitution

The unauthorized substitution of one stored key for another, whether encrypted or unencrypted, *must* be prevented. This precaution reduces the risk of unauthorized persons substituting keys known only to them.

When it is not feasible to physically or cryptographically prevent the substitution of one encrypted stored key for another, it *must* not be possible for an adversary to ascertain cleartext and corresponding ciphertext encrypted under the ZCMK. In addition, such substitution can be cryptographically prevented by encrypting the stored key as a function of the users' identities (for example, XORing the users' identities with the ZCMK before encrypting the stored key). Also, if the compromise of any key is known or suspected, both the keys in question and their KEK *must* be changed.

Restrictions on Use of PIN Protection Keys

A key used to encrypt a PIN or protect the PIN Encryption Key *must* never be used for any other cryptographic purpose. Variants of the same key, however, can be used for different purposes.

Limiting the Effects of Key Compromise

The following requirements are necessary to prevent the compromise of the key or keys in one cryptographic device from compromising the encryption keys in any other cryptographic device:

- Any ZCMK and PIN Encryption Key used to encrypt the transaction PIN in other than a PIN entry device *must* be known only at two locations: where the key or PIN is encrypted and where it is decrypted.
- Any key used to encrypt a PIN in a minimum acceptable PIN entry device *must* be known only in that device and in security modules at the minimum number of facilities consistent with effective system operations.
- No cryptographic key *must*, except by chance, be equal to any other cryptographic key. Knowledge of one cryptographic key *must* provide no information about any other cryptographic key, except in the case of a variant of a key, the irreversible transformation of a key, or keys encrypted under a key.

- The irreversible transformation of a key *must* be used only at the same level in a key hierarchy as the original key or the level immediately below that of the original key.
- The variant of a key *must* be used only in those devices that possess or possessed the original key.

Key Replacement

A cryptographic key *must* be replaced with a new key whenever the compromise of the original key is known or suspected. The replacement key *must* not be a variant of the original key, nor an irreversible transformation of the original key. In addition, all keys encrypted under or derived using that key must be replaced with new keys within the minimum feasible time.

A cryptographic key *must* be replaced with a new key before it is feasible to determine the key through exhaustive attempts.

Key Destruction

Keys that are no longer used or that have been replaced by a new key *must* be destroyed. This precaution is necessary because any information that was encrypted under the old key can be decrypted and the contents revealed.

All keys *must* be securely destroyed as follows:

- If the key is maintained on paper, the key is to be destroyed by burning or shredding.
- If the key is stored on an EEPROM, the key should be overwritten with binary zeros a minimum of three times. If the key is stored on an EPROM or PROM, the chip should be smashed into many small pieces and scattered.

In all cases, keys *must* be destroyed by another individual other than the key custodian. An affidavit must be signed by all parties observing this destruction process. This affidavit is kept indefinitely with the key log.

Procedure Documentation

To ensure a high level of security and integrity, documented procedures and controls *must* exist for managing PINs, keys, and security systems. This section lists the minimum acceptable standards for providing adequate controls and documentation requirements.

PIN Management and Security Procedures

All procedures related to PIN entry, transmission, storage, and verification *must* outline the controls for preventing or detecting the compromise of PINs.

PIN Entry

PINs that are not encrypted *must* be within a TRSM or within a minimum acceptable PIN entry device. Procedures for certifying TRSMs and minimum acceptable PIN entry devices *must* be documented.

Procedures *must* be documented and used to detect the tampering with or loss, theft, substitution, or unauthorized modification of PIN-processing equipment.

If a TRSM can translate a PIN from one PIN block format to another, or if the TRSM verifies PINs, then procedures and controls *must* be documented and in place to prevent or detect repeated, unauthorized calls resulting in the exhaustive determination of PINs.

The procedures to follow when the suspicious alteration of a key in a TRSM is detected must be documented. This precaution ensures that new keys are not installed in the equipment until it has been inspected and a reasonable degree of assurance has been reached that the equipment has not been subject to unauthorized physical or functional modification.

PIN Transmission

The PIN block formats used *must* be documented. If double-length keys are used for PIN encryption, procedures detailing the method and sequence for encrypting with the double-length key also *must* be documented.

Criteria for rejecting the encrypted PIN block *must* be documented. This procedure should identify when rejection would occur (for example, decryption, reformatting, re-encryption) and what condition would cause the rejection (for example, the Control field is not binary 0000).

Additionally, procedures for changing the security system software used for PIN transmission and translation *must* be documented.

PIN Storage

SMS members *must* document procedures for transactions that are stored or stored and forwarded. These procedures should include the conditions of storage and the method used to protect the PIN.

PIN Verification

The methods used for PIN verification must be documented.

Key Management and Security Procedures

All procedures related to key creation, transmission, loading, and administration *must* use access logs and be carried out in a physically secure environment. Access to TRSMs *must* be controlled and logged.

Key Creation

Procedures for creating keys *must* be documented. This process includes documenting zone definition, the key hierarchy used, and how key uniqueness is ensured. A process for requesting the generation of ZCMKs and Working Keys and the physical security during the creation of the key components *must* be documented. Additionally, procedures used for changing the security system software used for key creation *must* be documented.

Key Transmission

Procedures for transferring separate hardcopy components of a key or transmitting the ciphertext form of a key *must* be documented. Application of the principles of dual control and split knowledge should be documented, including the process of identifying and selecting employees to be entrusted with key custodial responsibilities.

Key Loading

Procedures for loading separate hardcopy components of a key *must* be documented and followed. The physical security measures used when loading keys into TRSMs or minimum acceptable PIN entry devices, and the application of the principles of dual control and split knowledge during the loading of the key components or during key injection into PIN entry devices, *must* be documented.

Key Administration

Procedures describing how keys are protected from disclosure and key substitution *must* be documented. If Dynamic Working Key Exchange or key variants are used, when and how they are used *must* be documented.

Procedures for detecting key compromise and the process for replacing a compromised key with a new key *must* be documented.

Procedures for destroying keys that are no longer used or that have been replaced by new keys *must* be documented. Documentation should include the method of destruction and confirmation of destruction.

Self-Audit Procedures

Participants in the electronic interchange system must comply with the standards presented in the *Consolidated PIN Security Standards Requirements*. To measure compliance, each participant in the transaction processing chain who manages cardholder PINs and encryption keys *must* complete the Consolidated PIN Security Standards Self-Audit, in *Consolidated PIN Security Standards Requirements*.

Proprietary and processor members are responsible for verifying that their member group, as a whole, is in full compliance. It is the responsibility of the designated auditing staff of each member group to explore the possible security implications of each unique implementation.

Security Self-Audit

The Consolidated PIN Security Standards Self-Audit and compliance statement (found in *Consolidated PIN Security Standards Requirements*) *must* be completed and returned 45 days before the advent of card activation or card processing, or both. Completion of the full self-audit and compliance statement is required every third year thereafter.

Any time a participant makes substantive security changes, revalidation is required. A new security self-audit *must* be completed within 45 days of such changes.

Annual Certification

In the years that the self-audit is not performed, the participant *must* complete and return an annual certification form (found in *Consolidated PIN Security Standards Requirements*). The certification verifies that there have not been substantive changes to the participants' last security self-audit.

The annual certification statement is required at the end of the quarter for the month that the full security self-audit was completed. For example, if the participant completes the self-audit in February, the annual certification would be required by March 31 of the next year, and thereafter.

Audit Exception Form

For every answer that is not "yes," an audit exception form *must* be completed. The audit exception form identifies why the participant is not in compliance and what actions are being taken to bring the participant into compliance. A blank form is in *Consolidated PIN Security Standards Requirements.*

When compliance is not possible, the interchange network contacts the member to review and resolve any exceptions.

Auditor Verification

The Consolidated PIN Security Standards Self-Audit is to be completed and certified by an internal or independent auditor. The auditor *must* have sufficient skill and experience to determine compliance.

Field Review

The interchange network, at its discretion, can perform an on-site inspection to verify the participant's compliance to the security self-audit. All auditor work papers from the self-audit can be requested and should be kept for a minimum of three years. A complete audit form is in *Consolidated PIN Security Standards Requirements.*

Routing 8

Routing refers to decisions made when sending transactions from the acquirer to SMS and from SMS to the issuer.

This chapter includes a description of:

- How SMS determines transaction routing from one member to another.
- The routing services available for both acquirers and issuers.

Transaction Routing

To route transactions, SMS maintains information on Network IDs, card types, account ranges, and processors. For example, SMS usually routes cardholder transaction requests based on the account number in the message.

Table 8–1 lists each SMS transaction and on what field the routing decision is based.

Table 8–1: SMS Transaction Routing

Transaction	Message Type	Routing Decision Based on...
Preauthorization	0100	The account number contained in Field 2—Primary Account Number.
Purchase Merchandise Credit POS Cancellation Store and Forward Resubmissions	0200	
Reversal	0420	
Adjustment, Representment	0220	
Chargeback	0422	The acquirer ID contained in Field 32—Acquiring Institution Identification Code.
Text Messages	0600	The member identified in Field 100—Receiving Institution Identification Code.

Routing Options, Table, and Services

Routing options are determined by issuers and acquirers. This section discusses the following items:

- Interlink Routing Table
- Priority Routing Service
- Alternate Routing Service

The following routing services also are available to Interlink acquirers and are discussed in the *V.I.P. System Services* manual:

- Check Acceptance Service—This service allows merchants to use SMS routing for the submission of check approval requests to selected check acceptance vendors.
- Gateway Services—VisaNet has connections, or gateways, to various systems and networks. Gateway Services link acquirers accepting non-Visa card products and services to other networks outside of VisaNet. through the same connections used for Visa transactions.

Interlink Routing Options

For Interlink members, the Alternate Routing and Priority Routing services are optional for acquirers and issuers. The Interlink Routing Table is mandatory for acquirers.

In addition, to help acquirers determine whether a cardholder's bank is participating in Interlink, Visa provides acquirers with a file of participating BINs. Acquirer and merchant systems can check this file before submitting a transaction for Interlink. Routing service options described in this chapter are shown in Table 8–2.

Table 8–2: Interlink Routing Table and Service Options

Routing Table and Services	Acquirer	Issuer
Interlink Routing Table	Mandatory	
Priority Routing	Optional	
Alternate Routing	Optional	Optional

Interlink acquirers must use the Interlink Routing Table and must specify *either* of the following in Field 63.1—Network ID:

- The preferred card program they wish to participate in (for example, Network ID 0002=Visa, 0003=Interlink).
- A value of 0000, if they wish to participate in the Priority Routing service. For more information about Priority Routing, see the "Priority Routing" section later in this chapter. Before participating in Priority Routing, members must contact their Visa representatives.

Interlink Routing Table

The Interlink Routing Table enables Interlink acquirers to receive a VisaNet-generated Interlink Routing Table in file or report form. The table is distributed weekly and identifies valid Interlink account number ranges. Acquirers use this information to make authorization routing decisions.

The Interlink Routing Table is available in two automated formats:

- Routing file
- Routing report

Acquirers have the option to receive one or both versions of the Interlink Routing Table.

Interlink Routing Table File—This batch data file lists all Interlink card prefixes, prefix lengths, account number lengths, issuers' country codes, and issuing members' names. The file helps Interlink acquirers determine which account ranges belong to Interlink issuers. VisaNet transmits this batch data file to the acquirer's VisaNet Access Point (VAP) on a weekly basis. See Chapter 11, Member-to-Visa Connection Options, for file identification information.

Interlink acquirers may share the file with merchants. Merchants may want to ensure that a card number is in the table before accepting the risk of a store-and-forward transaction.

Acquirers can request a retransmission of the file. Acquirers requesting a retransmission receive a duplicate of the most recently transmitted file. Earlier versions of the file are not available.

Each new file completely replaces the previous file. The file includes a single header record, multiple data records (one data record for each unique card prefix, account number length combination, or both), and a single trailer record. The header and trailer records are used for file validation and are not intended to be part of the file used by acquirers' host systems. See files appendix of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*, for file layouts and additional information on how to use the file.

A member separator program is required to generate the final routing table for use by the acquirer. A sample program is provided in the files appendix of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications*. The files appendix also provides specifications for the header, data, and trailer records. The format is based on the format of the Plus BIN Table.

Interlink Routing Table Report—This report lists all Interlink card prefixes, prefix lengths, account number lengths, issuers' country codes, and issuing members' names. The report consists of two subreports:

- The first contains the updates that have occurred since the previously distributed report.
- The second contains all BIN card prefixes supported for Interlink transactions.

The report is delivered to members electronically in print line format.

Routing Services

This section discusses each of the routing services.

Priority Routing

Acquirers that process two or more card products on SMS can use the Priority Routing Service. The service allows SMS to determine which network and card program rules to apply to message routing decisions for preauthorizations, financial messages, and their reversals.

Acquirers can invoke Priority Routing by placing "0000" in Subfield 63.1—Network ID. Upon receipt of the request, SMS compares the networks of the acquirer and the issuer, identifies a common network, and routes the message accordingly. If SMS detects more than one common network, it selects the network preferred by the acquirer (a value stored by SMS).

SMS assigns the appropriate network ID and then forwards the request to the issuer with only those fields that pertain to the network's programming rules.

SMS includes the assigned network ID in the response to the acquirer.

NOTE: *If an acquirer wants a transaction to be processed for a particular network, the acquirer should use the appropriate network ID; for example, Network ID 0002=Visa, 0003=Interlink.*

Alternate Routing

To determine routing, SMS maintains information on network IDs, account ranges, processing centers, acquirer and issuer stations, and user preferences. Both acquirers and issuers can designate an alternate endpoint to originate or receive (or both originate and receive) exception transactions and other back office transactions.

The alternate endpoint can be located at the participant's site or another site, and use either the Visa BackOffice Adjustment System (BOAS) or an equivalent back office system. For information about BOAS, see the list of BOAS documents in the About This Manual chapter.

Transactions eligible for Alternate Routing Service include:

- Paper sales drafts.
- Adjustments and back office adjustments.
- Chargebacks.
- Representments.
- Administrative messages, including free text.
- Updates to the Exception File, PIN Verification File, or both.

Only issuers or their designates can update the Exception and PIN Verification files.

For exception transactions and administrative messages, different endpoints can be specified for Interlink and ATM transactions. An alternate endpoint can be used for Interlink transactions only, ATM transactions only, or both.

If two alternate endpoints are specified, one is used for ATM transactions and the other is used for Interlink transactions.

Alternately routed transactions can be settled at an alternate settlement entity. An alternate settlement entity can be specified only for alternately routed transactions.

Settlement and Reconciliation 9

The SingleConnect settlement and reconciliation process for Visa and Visa Electron is described in the following sections:

- Settlement Overview
- VisaNet Settlement Service (VSS) (VSS)

Settlement Overview

The settlement process consists of various tasks that are performed so that funds can be transferred. Settlement tasks are performed during and after transaction processing (clearing), the process that delivers transaction data to participants.

The settlement process includes the following tasks performed by VisaNet:

- Accumulating transaction counts and amounts during transaction processing
- Calculating a net amount for the settlement day after transaction processing
- Reporting the net amount to a funds-transfer agent that manages the actual debit or credit to participants' settlement accounts

When transactions are processed through SMS, they are delivered for account posting in real time through the use of 02*xx* and 04*xx* messages. Thus, settlement refers to accumulating these transaction counts and amounts and then determining the net amount to be transferred to and from the participant's settlement account.

Transactions Qualifying For Settlement

All SingleConnect financial transactions are settled by VisaNet. A transaction qualifies for settlement if it meets the following criteria:

- The account number must be within account ranges belonging to a SingleConnect issuer set up for SMS participation
- The transaction must be one of the following types of financial transactions:
  - Preauthorization completions
  - Purchases
  - Cash disbursements
  - Financial transaction reversals
  - Cancellations at point of sale
  - Downtime resubmissions (electronic or paper-based)
  - Chargebacks
  - Representments
  - Adjustments

Values of the following transactions are not included in settlement totals; however, processing charges apply and are billed at month end.

- Balance inquiries
- Declined financial transactions

Settlement Day

Settlement accumulation and reporting are done daily; however, funds transfer occurs only on banking days. Thus, the term *settlement day* refers to a 24-hour period during which transactions are accumulated. At the end of a settlement day, accumulators are cleared, the system settlement date is advanced, and reports are prepared.

The Gross Interchange Value (GIV) is reflected on daily reports. Each banking day, the net settlement amount for the settlement day is wire-transferred to or from the participant's settlement account. For non-U.S. dollar settlement, the wire transfer occurs two business days after the processing date.

NOTE: *If a member processes BASE II as well as SMS messages, SMS and BASE II settlement can be combined in one wire transfer. To exercise this option, contact your Visa representative.*

Accumulation and Reconciliation

As transactions occur, SMS logs them and accumulates counts and gross amounts of those qualifying for settlement. At the end of the settlement day (EOD), accumulated totals are placed in 0520 reconciliation advices. The advices contain the number and value of transactions accumulated since the beginning of the settlement day.

End-of-day (EOD) 0520 reconciliation advices are optionally delivered automatically when participants sign on to recovery status. For details see the "Network Management Transactions" section of Chapter 4, Message Types and Flows.

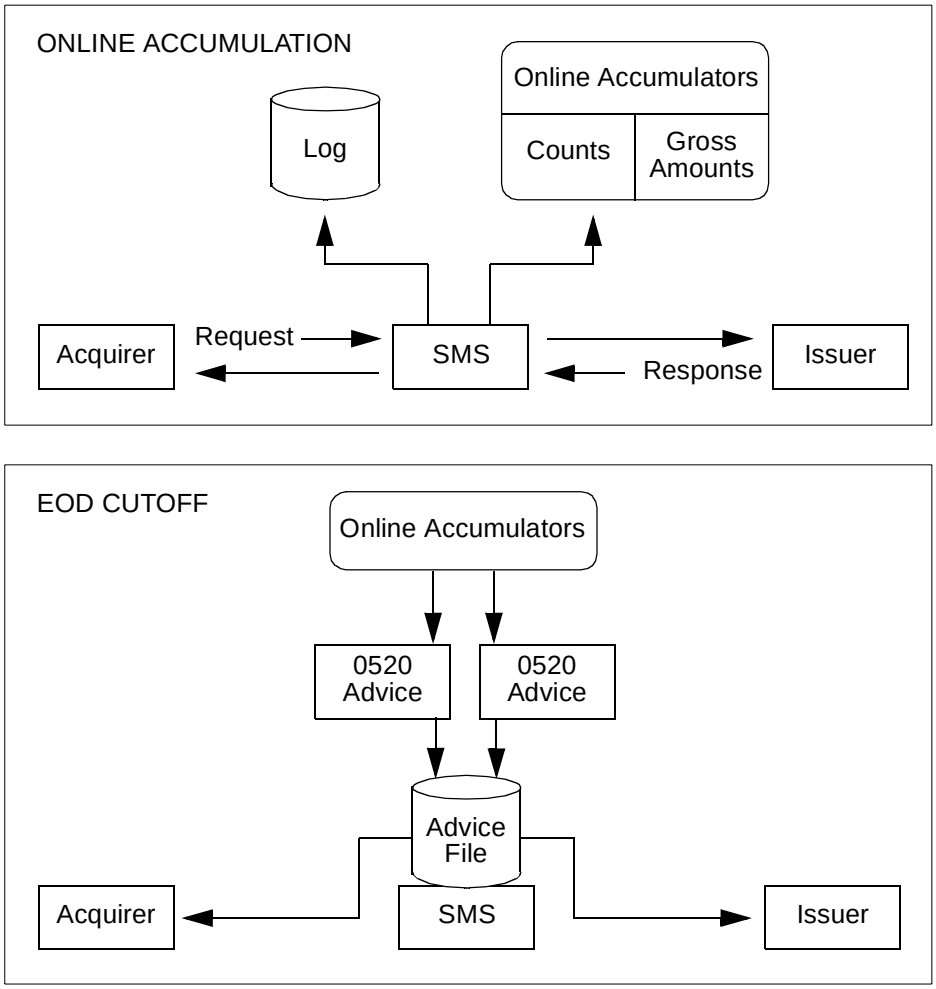
In addition, members can request 0500 reconciliation advices that contain the cumulative settlement totals for the day, from start of processing to the time of the request for the advice.

To exercise these options, contact your Visa representative.

After advices are recovered, they can be used to cross-check acquirer center and issuer totals with those accumulated by SMS.

Figure 9–1 outlines the accumulation and advice generation processes.

Figure 9–1: Overview of Online Process



Offline Processing

At the end of the settlement day, an SMS offline process uses the logged data to total the transactions processed.

The result of this process is a net settlement value for each settlement endpoint and the production of daily settlement reports.

Transactions for each settlement day are accumulated throughout the monthly cycle. Pertinent information is held to produce month-end bills for processing charges. All chargebacks, representments, and adjustments processed during the cycle are held and used to produce monthly exception transaction compliance reports.

VisaNet Settlement Service (VSS)

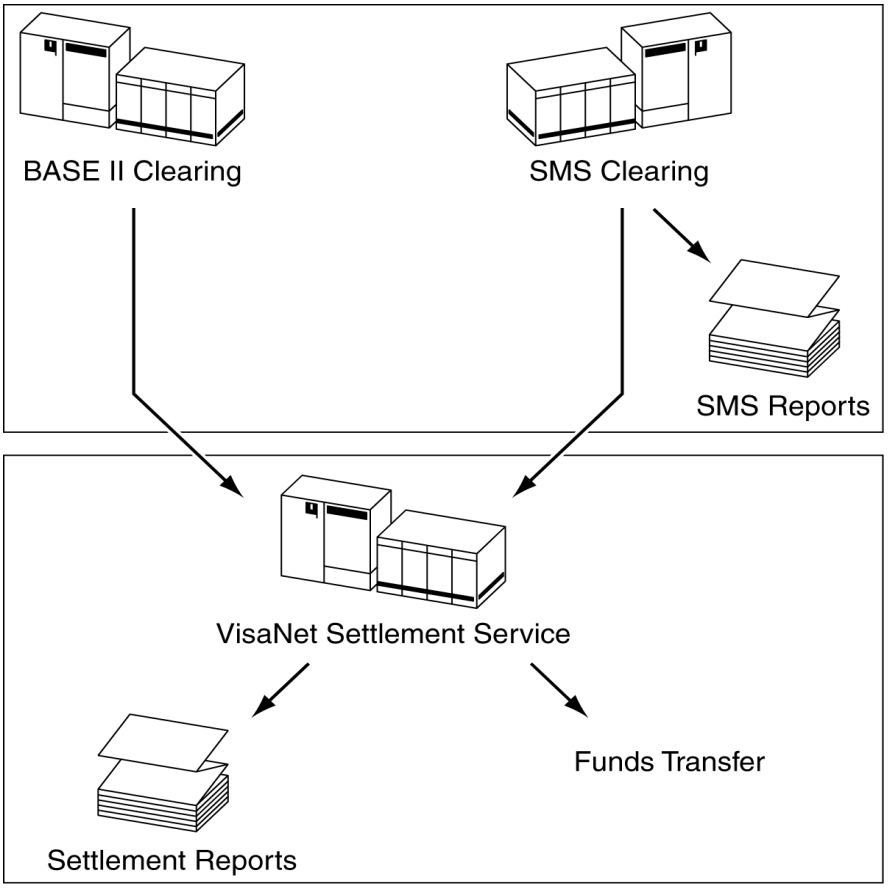
SingleConnect members settle through the VisaNet Settlement Service. Visa processes interchange transactions for SMS and BASE II through separate systems. Both SMS and BASE II perform their own clearing functions. VSS performs the settlement functions for SMS and BASE II in one centralized service that ensures consistency in settlement and reporting.

Clearing and settlement are defined as follows:

- Clearing is the process of collecting an individual transaction from one member or processor and delivering it to another.
- Settlement is the process of calculating and determining the net financial position of each member for all transactions that are cleared.

The VSS clearing and settlement process is shown in Figure 9–2.

Figure 9–2: VisaNet Settlement Service (VSS) Process



VSS provides members with the following features:

- Flexibility in establishing settlement relationships
- Standardized report layouts in print-ready and machine-readable formats
- Several report delivery options
- Member-defined funds transfer points
- Choice of settlement options for alternately-routed transactions

The following sections describe these features along with key elements of the settlement and reconciliation process in the VSS environment.

Settlement Services

Within VSS, Visa offers two settlement services:

- International Settlement Service
- National Net Settlement Service

The International Settlement Service is used to settle all international transactions and domestic transactions for members that do not participate in a National Net Settlement Service.

The National Net Settlement Service allows members within a country to settle qualifying domestic transactions through a central settlement agent bank. Qualifying transactions are those for which the merchant, acquirer, and issuer are in the same country, and the transaction currency is the local currency for that country.

Settlement Relationships

VSS provides flexibility when defining settlement relationships.

Members can define up to eight levels of settlement relationships in a hierarchy of settlement reporting entities (SREs).

The different levels allow members to build and maintain the most appropriate settlement relationships for their business needs. For example, the settlement relationship levels can be used to reflect the products in a member's organization. With this flexibility, members can easily and efficiently manage settlement functions.

Settlement Schedule

The cutoff time for SingleConnect Visa and Visa Electron transactions processed by VisaNet is shown in Table 9–1 in Greenwich mean time (GMT). The GMT cutoff time changes by one hour when times change because of daylight savings.

IMPORTANT

Visa is enhancing the Single Message System (SMS) and BASE II to more closely synchronize processing between the systems. These enhancements will:

- *Enable BASE II to clear transactions seven days per week, instead of the current six.*
- *Synchronize the settlement cutoffs for SMS and BASE II, resulting in a standard cutoff time of:*
  - 10 GMT from first Sunday in April to last Sunday in October.
  - 11 GMT from last Sunday in October to first Sunday in April.

14 July 2001 is the planned installation date for these enhancements, which will be mandatory for all SMS and BASE II members.

Table 9–1: Settlement Cutoff Timing—SingleConnect Interlink Transactions

GMT Dates	GMT
First Sunday in April to last Sunday in October	0300
Last Sunday in October to first Sunday in April	0400

Other key times in the daily settlement process are shown in Table 9–2.

Table 9–2: Daily Settlement Process

Event	GMT	
	Apr – Oct	Oct – Apr
Settlement report processing and report delivery begins	1000	1100
Delivery of SMS reports and raw data to VisaNet endpoints completed	1500	1600
Reporting of net settlement positions to the National Settlement Banks for domestic transactions	1500	1600
Delivery of funds transfer positions to the Visa Settlement Bank completed	1630	1730

The relative timing of these events is summarized in Table 9–3.

Table 9–3: Timing of Settlement Process (GMT)

	For work of						
	Mon	**Tue**	**Wed**	**Thu**	**Fri**	**Sat**	**Sun**
SMS detail reports and raw data delivered seven days a week	Tue	Wed	Thu	Fri	Sat	Sun	Mon
VSS summary reports prepared and delivered seven days a week	Tue	Wed	Thu	Fri	Sat	Sun	Mon
Funds transfers for US$ settlement	Tue	Wed	Thu	Fri	Mon	Mon	Mon
Funds transfers for non-US$ settlement	Thu	Fri	Mon	Tue	Wed	Wed	Wed

Alternately Routed Transactions

Members can use an alternate processor, such as the BackOffice Adjustment System (BOAS), to collect and deliver exception transactions and other back office transactions. For SingleConnect members, this option is called alternate routing.

Members can specify whether to settle these transactions with their normally routed transactions or separately.

Funds Transfer

This section describes:

- SMS messages containing settlement-totals data.
- The movement of actual funds.

SMS 0620 Funds Transfer Messages

After the completion of settlement, SMS uses 0620 advices to send the day's final funds transfer totals (but not the funds themselves) to issuers and acquirers. For more information about these advices, see "Funds Transfer Message" in Chapter 4.

Movement of Funds

The final step in the settlement process is the actual funds transfer, during which funds are collected from settlement entities with a net debit position and paid to settlement entities with a net credit position.

Funds transfer refers to the movement of funds between the member's settlement bank and Visa's settlement bank for the purpose of settlement. Funds transfers are a net of the member's credits and debits.

Funds can be settled in U.S. dollars (USD) or non-USD currency with a member-selected settlement bank.

Each funds transfer is associated with only one settlement account, although several funds transfers can be associated with the same account.

Funds Transfer Point

The funds transfer point can be defined at any level in the settlement structure. This flexibility allows members using third-party processors to be responsible for their own funds transfers.

VSS Reports

VSS offers control over settlement reporting and the ability to send reports to multiple locations.

Layouts and Formats

VSS reports provide a common layout for BASE II and SMS members. This common layout allows all members to streamline their internal procedures. It eliminates the need to cross-train personnel on different back office reconciliation layouts for SMS and BASE II settlement reports.

All VSS reports are available in both print-ready and machine-readable formats. Receiving reports in machine-readable formats allows members and processors to:

- Provide automated interfaces to internal systems.
- Automate their reconciliation process.

To reflect the business needs of members, VSS reports use common, business-oriented terminology, which makes them easy to read and reconcile.

Delivery

Members can have their reports sent to multiple locations of their choice, including locations other than their processing centers. Interchange routing does not determine the routing of settlement information.

Reconciliation

SingleConnect members and processors must be able to reconcile their internal totals to those provided by VisaNet. VSS is designed to help members meet each of the following reconciliation requirements:

- Match counts and amounts of financial transactions cleared by VisaNet
- Match counts of nonfinancial transactions cleared by VisaNet
- Match counts and amounts of transactions sent to or received from VisaNet for settlement with members' and processors' settlement totals
- Find specific fields on the VisaNet Settlement Service (VSS) reports that are needed for reconciliation

Key elements of the reconciliation process include:

- Processors and VSS settlement hierarchies.
- Reports and files.
- SMS reconciliation messages.

These elements are described in the following sections.

Processors and VSS Settlement Hierarchies

Effective reconciliation procedures are based on the relationships between processors and VSS settlement hierarchies. Possible relationships include:

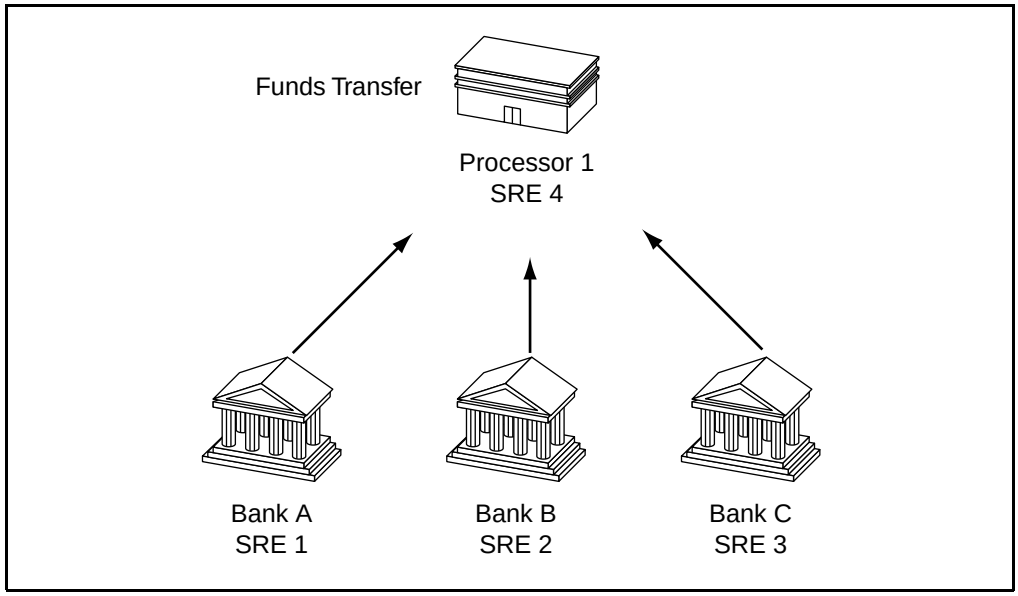
- Processor performs funds transfer for all members.
- Processor performs funds transfer for some members and not others.
- Processor supports National Net Settlement Service transactions.

Such hierarchies are reflected in the reports and files used in the reconciliation process.

Figure 9–3 contains an example of a settlement hierarchy, where a processor performs funds transfer for all its members. In this case, Processor 1 (SRE 4) represents:

- The funds transfer totals for Banks A, B, and C.
- The total work performed by the processor.

Figure 9–3: Settlement Hierarchy Example—Processor Performing Funds Transfer for All Members



Reports and Files

SingleConnect members and processors can reconcile their daily activity using the following reports and files:

- VSS reconciliation reports—VSS reconciliation reports provide totals for all transactions sent to or received from VisaNet, including nonfinancial transactions.
- VSS settlement reports—VSS settlement reports provide interchange, reimbursement fee, and charge totals settled by VSS.
- SMS transaction detail reports—Optional SMS transaction detail reports provide an audit trail of all SMS transactions in the day's settlement total. The reports can be used to research differences, if any, between totals reported by VisaNet on the VSS reports and those reported by the member's or processor's system.
- Raw data files—Raw data files can be used, in conjunction with VSS machine-readable reports, to automate the reconciliation process.

  As an optional service, Visa provides raw data files that contain detailed information about the settlement day's transactions for a given participant. Raw data is available to all SingleConnect issuers and acquirers. Users of this service can use the data to create customized reports and to reconcile data reported by their own systems.

  Raw data is distinguished from report data in that it is suited for automated processing. The raw data records are produced from the same sources as SMS reports.

SMS Reconciliation Messages

In addition to using the reports mentioned in the previous subsection, SingleConnect members can optionally reconcile their online activity by using SMS reconciliation (0500 and 0520) messages that contain the current or previous day's gross interchange totals (that is, the financial position exclusive of fees and charges) accumulated online. Each message contains the counts and amounts accumulated by VisaNet for approved, settled transactions.

Online totals are accumulated at the processor level. The processor's totals include the totals of each affiliate. These messages can be used by a processor to balance its online totals to the totals accumulated by VisaNet.

An 0520 message is generated for each settlement currency. Totals are accumulated separately for International Settlement Service and National Net Settlement Service transactions. A processor whose International Settlement Service and National Net Settlement Service transactions are in the same settlement currency has the option of getting reconciliation messages that include a combined total.

For More Information

For detailed information about the VSS topics discussed in this section, please refer to the *VisaNet Settlement Service (VSS) User's Guide.*

NOTE: *Raw data record layouts are available in both the* VisaNet Settlement Service (VSS) User's Guide *and the* V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications.

Interlink Exception Processing and Dispute Resolution 10

Exception processing and dispute resolution allows members to resolve problems, respond to customer inquiries, and provide information to other Interlink participants.

All Interlink participants, whether issuers or acquirers, or both, must be thoroughly familiar with exception processing and dispute resolution and be able to handle both processes in a timely and accurate manner.

This chapter provides information about:

- Exception processing and dispute resolution functions required for both issuers and acquirers.
- Exception processing system design considerations.

Required Functions

Both issuers and acquirers must support the exception processing and dispute resolution messages as shown in Table 10–1.

Table 10–1: Required Exception Processing and Dispute Resolution Functions

Acquirer Requirements	Issuer Requirements
Acquirers must: • Create adjustment transactions. • Receive chargeback transactions. • Create representment transactions. • Create Interlink paper sales draft transactions (optional). • Create and receive administrative messages.	Issuers must: • Receive adjustment transactions. • Create chargeback transactions. • Receive representment transactions. • Receive paper sales draft transactions. • Create and receive administrative messages.

All Interlink exceptions are supported through online messages. Members can develop their own system capabilities or use the BackOffice Adjustment System (BOAS).

This chapter also discusses the processing of paper sales drafts. Paper sales drafts are optional transactions for acquirers, but they must be supported by issuers.

Issuer Exception Processing and Dispute Resolution

Exception processing and dispute resolution for issuers is primarily used to correct errors reported by cardholders. Exception processing also is used to resolve settlement exceptions.

To process exceptions, issuers initiate chargebacks and administrative messages and receive adjustments and representments.

After the customer service staff has completed internal research and determined that additional information is required to resolve a problem or that a cardholder's original purchase was invalid, the staff can initiate a chargeback or administrative message.

Chargebacks

In general, a chargeback can be initiated when:

- A cardholder claims a transaction posted to his or her account was processed more than once.
- A cardholder claims a transaction posted to his or her account was processed in error, such as for a wrong amount.
- A cardholder disputes a transaction that was authorized as an Interlink paper sales draft transaction.
- A transaction was processed at a time when the merchant was classified as a "special merchant." Special merchant considerations are discussed in the Interlink operating regulations.
- An adjustment received from an acquirer is designated for posting to a closed account or an account that does not have sufficient funds (NSF).
- A merchandise credit was not posted to a cardholder's account.

After receiving a cardholder's claim of error or inquiry, or identifying an error in reconciliation, the issuer completes research of internal records and Interlink settlement reports to determine if the inquiry or error can be resolved with data available in-house. If the issuer concludes that the original transaction is an acquirer responsibility, the issuer initiates a chargeback.

Interlink operating regulations provide specific reasons for chargebacks and time frames for returning transactions to acquirers. Acquirers can re-present (return) chargebacks considered invalid. Following a representment, an issuer must not charge back the transaction a second time. An Interlink issuer may have the right to file for arbitration after receiving a representment.

The chargeback amount can be less than the amount of the original transaction. If the chargeback amount is different from the original transaction amount, then Field 61.1—Other Amounts contains the original transaction amount.

When submitting a chargeback, issuers identify the original transaction to the acquirer by returning some of the original data elements in the chargeback request. Issuers must be able to provide the information in the following fields from the original purchase transaction:

- Field 2—Primary Account Number
- Field 13—Date, Local Transaction
- Field 18—Merchant's Type
- Field 19—Acquiring Institution Country Code
- Field 20—PAN Extended, Country Code (if provided in the original request)
- Field 32—Acquiring Institution Identification Code
- Field 33—Forwarding Institution Identification Code (if provided in the original request)
- Field 37—Retrieval Reference Number
- Field 42—Card Acceptor Identification Code
- Field 43—Card Acceptor Name/Location
- Field 49—Currency Code, Transaction (value from either field 50 or 51 from the original transaction; reflects the current amount in field 4 of the chargeback)
- Field 59—National POS Geographic Data (required only for the U.S. and Canada Visa regions)
- Field 63.1—Network Identification (For Interlink transactions, the network ID is 0003.)
- Field 63.11—Reimbursement Attribute

In addition, tracing information from the original transaction is provided separately in Field 90—Original Data Elements and in Field 125—Supporting Information. Tracing information includes the Message Type, Systems Trace Audit Number, and Transmission Date and Time.

Issuers submitting chargebacks can use the value in Field 11—Systems Trace Audit Number from the original purchase transaction, or they can assign a new value. Issuers must assign a new value for Field 7—Transmission Date and Time. The new value is the time of day in Greenwich mean time (GMT) when the chargeback transaction is submitted to the VisaNet Integrated Payment (V.I.P.) System.

Table 10–1 shows the information that must be provided in Field 90—Original Data Elements and in Field 125—Supporting Information.

Table 10–1: Data in Field 90 and Field 125 for Chargeback Transactions

Data	Field 90	Field 125
Reimbursement Attribute	n/a	Reimbursement Attribute from field 63.11 of the original 0200 or 0220 transaction, followed by a "/" (slash)
Original Message Type	Message Type from original 0200 or 0220 transaction; mandatory.	n/a
Original Trace Number	Systems Trace Audit Number from field 11 of the original 0200 or 0220 transaction; mandatory.	Duplicate from field 90.
Original Transmission Date and Time	Transmission Date and Time (GMT) from field 7 of the original 0200 or 0220 transaction; mandatory.	Duplicate from field 90.
Original Acquiring Institution Identification Code	Acquiring Institution Identification Code from field 32 of the original 0200 or 0220 transaction; optional.	n/a
Original Forwarding Institution Identification Code	Forwarding Institution Identification Code from field 33 of the original 0200 or 0220 transaction; optional.	n/a
Unformatted Text	n/a	Explanatory text is mandatory when the message reason code in field 63.3 is: • 2480 • 2483 • 2484 • 2498 (See Table 10–2 for requirements for explanatory text for transactions with the above message reason codes.) Explanatory text is optional when the message reason code is: • 2493 • 2494 • 2496

Table 10–2 shows the information that must be provided in the Unformatted Text subfield of Field 125—Supporting Information.

Table 10–2: Requirements for Explanatory Text in Field 125

Message Reason Code (in Field 63.3)	Text Requirements
2480	Based upon invalid or unpostable adjustment • Field 11—Systems Trace Audit Number of adjustment • Field 7—Transmission Date and Time (GMT) of the adjustment • Explanation of chargeback (for example, account closed, nonsufficient funds, or invalid data)
2483	Based upon credit not received with merchandise receipt • Field 11—Systems Trace Audit Number from receipt • Date from receipt • Time from receipt
2484	Based upon credit not received without merchandise receipt • Field 11—Systems Trace Audit Number (can be zero-filled) • Date of merchandise credit • Time of merchandise credit (if available; otherwise, can be zero-filled)
2498	Based upon processing error Free text, clear explanation of the processing error
2487 (U.S. region only) 2493 2494 2496	Free text (optional)

Table 10–3 summarizes processing specifications for Interlink chargeback transactions, as specified in the Interlink operating regulations.

Table 10–3: Processing Specifications for Chargeback Transactions (1 of 2)

Chargeback Reason	Usage	Time Frame	Documentation or Information Required	Message Reason Code (in Field 63.3)
Invalid or unpostable adjustment	The adjustment contains invalid data or is for posting to a closed or NSF account.	Within 10 calendar days of adjustment transaction date.	No documentation required. The chargeback transaction must contain the transmission date and time, trace number of the disputed transaction, and an explanation of the chargeback reason.	2480
Credit not received with receipt	To charge back an original purchase because a merchandise credit has not been received and posted by the issuer. The cardholder has the merchandise credit receipt.	Within 100 calendar days from the merchandise credit transaction date, but only after 10 calendar days from the merchandise credit transaction date have elapsed.	The chargeback transaction must contain the transmission date and time, and the trace number of the original transaction. The information is obtained from the receipt for the merchandise credit.	2483
Credit not received without receipt	To charge back an original purchase because a merchandise credit has not been received and posted by the issuer. The cardholder does not have the merchandise credit receipt.	Within 100 calendar days from the merchandise credit transaction date, but only after 10 calendar days from the merchandise credit transaction date have elapsed.	The chargeback transaction must contain the transmission date and time, trace number of the original transaction, and the date of the merchandise credit transaction claimed by the cardholder.	2484
Nonreceipt of remote terminal merchandise	When the card issuer receives notification from the cardholder that merchandise was not received and the cardholder was charged	Within 100 calendar days from the transaction date, but only after 30 days from the transaction date have elapsed	n/a	2487

Table 10–3: Processing Specifications for Chargeback Transactions (2 of 2)

Chargeback Reason	Usage	Time Frame	Documentation or Information Required	Message Reason Code (in Field 63.3)
Special merchant	To charge back a transaction occurring during a time period in which the merchant has been classified as a special merchant by the Interlink Program Arbitration Committee.	Specified by the Interlink Program Arbitration Committee at the time of special merchant designation.	Specified by the Interlink Program Arbitration Committee at the time of special merchant designation.	2493
Unauthorized use	To charge back a downtime (Interlink paper sales draft) transaction that the cardholder claims was not authorized.	Within 100 calendar days of the latest posting of the Interlink transaction.	The chargeback transaction must contain the transmission date and time, and the trace number of the transaction or transactions.	2494
Duplicate processing	To charge back a transaction that is a duplicate of one already posted.	Within 100 calendar days of the latest posting of the Interlink transaction.	No documentation required.	2496
Processing error	When the cardholder notice of error is verified by the issuer. For example: the transaction was for a wrong amount or the cardholder received an invalid charge.	Within 100 calendar days of the latest posting of the Interlink transaction.	The chargeback transaction must contain the transmission date and time, and the trace number of the original.	2498

Administrative Messages

Issuers use administrative messages to:

- Request general information or additional transaction history from other members to properly process chargebacks.
- Respond to acquirer inquiries.

IMPORTANT

The issuer's operations staff must initiate administrative messages and respond to administrative messages from acquirers.

Acquirer Exception Processing and Dispute Resolution

Acquirers initiate adjustments and representments, as well as administrative messages. Acquirers can optionally submit paper sales drafts on their merchants' behalf. Additionally, the acquirer must respond to chargebacks and administrative messages from issuers.

Adjustments

Adjustments are transactions used by acquirers to correct processing errors that occur at the point of sale (POS). Adjustments also are used to correct out-of-balance conditions identified in acquirers' or merchants' settlement and reconciliation processes.

When acquirers receive settlement data from SMS and then complete the reconciliation process, they may identify transactions that, according to their records, are incorrectly settled with Visa. Following a similar reconciliation process between the acquirer and its merchants, transactions may be identified that are incorrectly settled. Acquirers research all such transactions using their internal records and SMS supplied reports and raw data before initiating adjustments.

Prompt use of adjustments by acquirers helps prevent cardholder disputes and chargebacks and also provides a basis for customer satisfaction in the product.

Correcting an error requires sending either a debit or credit adjustment to SMS to be delivered to the issuer.

EXAMPLE

- The acquirer requests a credit adjustment (Field 3—Processing Code equals 22*xxxx*) if a cardholder was overcharged, or if the issuer was charged for an invalid transaction, such as a transaction that was posted twice.

- The acquirer requests a debit adjustment (Field 3—Processing Code equals 02*xxxx*) if the cardholder was undercharged, for example, when a merchant keys in a transaction amount less than the actual sale amount.

Adjustment transactions are subject to several requirements:

- Adjustments are issued only on original transactions.
- Only one adjustment can be issued for an original transaction.
- Adjustments must be processed within 45 calendar days after the original transaction date. (The day after the purchase transaction is Day 1.) Adjustments submitted after 45 days are rejected unless they are designated as Good Faith Collections. Visa encourages acquirers to initiate adjustments as soon as errors are detected and verified.
- Adjustment transactions must include the fields required for Message Type 0220. Then processing code input (Field 3—Processing Code) by the acquirer indicates whether the adjustment is a debit or credit.

The adjustment transaction also must contain all of the information in the following fields from the original Interlink transaction:

- Field 2—Primary Account Number
- Field 32—Acquiring Institution Identification Code
- Field 37—Retrieval Reference Number
- Field 42—Card Acceptor Identification Code
- Field 43—Card Acceptor Name/Location
- Field 49—Currency Code, Transaction (value from either field 50 or 51 from the original transaction; reflects the current amount in field 4 of the adjustment)
- Field 59—National POS Geographic Data (if provided in the original request)
- Field 63.1—Network Identification
- Field 63.11—Reimbursement Attribute

In addition, information from the original transaction must be placed in Field 90—Original Data Elements and Field 125—Supporting Information, as shown in Table 10–4.

Table 10–4: Data in Field 90 and Field 125 for Adjustment Transactions

Data	Field 90	Field 125
Reimbursement Attribute	n/a	Reimbursement attribute from field 63.11 of the original 0200 or 0220 transaction, followed by a "/" (slash)
Original Message Type	Message Type from original 0200 or 0220 transaction; mandatory.	n/a
Original Trace Number	Systems Trace Audit Number from field 11 of the original 0200 or 0220 transaction; mandatory.	Duplicate from field 90.
Original Transmission Date and Time	Transmission Date and Time from field 7 of the original 0200 or 0220 transaction; mandatory.	Duplicate from field 90.
Unformatted Text	n/a	Merchant name and location; mandatory.

The adjustment transaction must assign a new value for the transmission date and time of the disputed transaction in Field 7—Transmission Date and Time. The acquirer can submit the trace number of the disputed transaction in Field 11—System Trace Audit Number or enter a new value.

Table 10–5 summarizes processing specifications for Interlink adjustment transactions, as specified in the Interlink operating regulations.

Table 10–5: Processing Specifications for Adjustment Transactions

Adjustment Reason	Usage	Time Frame	Documentation or Information Required	Processing Code Position 1 & 2 (of Field 3)	Message Reason Code (in Field 63.3)
Credit adjustment	Used by an acquirer to credit a cardholder for an incorrect difference of the actual charge.	Credit adjustments can be issued up to 45 days from the date of the original transaction.	No documentation required. The adjustment transaction must contain the transmission date and time, trace number of the transaction or transactions, and the merchant name and location.	22	2004
Debit adjustment	Used by an acquirer to charge an issuer for a transaction in which a cardholder was under-charged or not charged at all.	Debit adjustments can be issued up to 45 days from the date of the original transaction.	No documentation required. The adjustment transaction must contain the transmission date and time, the trace number of the transaction or transactions, and the merchant name and location.	02	2004

Good Faith Collections

Debit adjustments older than 45 days can be submitted and identified as Good Faith Collections. A value of GFC (for Good Faith Collection) in the first three positions of the Unformatted Text subfield of Field 125—Supporting Information must be used to identify the adjustment transaction as a Good Faith Collection.

Issuers have the right to dispute a Good Faith Collection transaction and submit a chargeback.

Representments

Representments are initiated by acquirers to resolve disputed chargebacks in which the original transactions were valid. That is, a representment is a transaction previously charged back to the acquirer, then presented again by the acquirer to the issuer.

Representments are used when:

- Chargebacks have been mis-sorted and the chargebacks were forwarded to the wrong acquirers.
- Acquirers have not received the required documentation or information for the chargebacks as stated in the Interlink operating regulations.
- Acquirers have provided documentation validating the original transactions.
- Acquirers have already issued adjustments to correct the original transactions.
- Merchandise credits have already been issued or are found to be invalid.

Acquirers must assign a reason code indicating why the chargeback is being represented. Documentation requirements are usually electronically included in the message, but can be required on paper. Interlink operating regulations specify documentation requirements for each reason code. Paper documentation, if required, must be supplied within 10 calendar days of the chargeback.

Acquirers must submit the representment with tracing information identifying both the original purchase transaction and the chargeback being disputed.

The representment transaction also must contain all of the information in the following fields from the original Interlink transaction:

- Field 2—Primary Account Number
- Field 3—Processing Code
- Field 4—Amount, Transaction
- Field 18—Merchant's Type
- Field 19—Acquiring Institution Country Code
- Field 20—PAN Extended, Country Code (if provided in the original request)
- Field 21—Forwarding Institution Country Code (required if Field 33 contains a "59" identifier)
- Field 32—Acquiring Institution Identification Code

- Field 33—Forwarding Institution Code (if provided in the original request)
- Field 37—Retrieval Reference Number
- Field 42—Card Acceptor Identification Code
- Field 43—Card Acceptor Name/Location
- Field 49—Currency Code, Transaction (value from either field 50 or 51 from the original transaction; reflects the current amount in field 4 of the original transaction)
- Field 59—National POS Geographic Data (required only for the U.S. and Canada Visa regions)
- Field 63.1—Network Identification (For Interlink transactions, the network ID is 0003.)
- Field 63.11—Reimbursement Attribute

In addition, information from the original transaction must be placed in Field 90—Original Data Elements and Field 125—Supporting Information, as shown in Table 10–6.

Table 10–6: Data in Field 90 and Field 125 for Representment Transactions

Data	Field 90	Field 125
Reimbursement Attribute	n/a	Reimbursement Attribute from field 63.11 of the original 0200 or 0220 transaction, followed by a "/" (slash)
Original Message Type	Message Type from chargeback transaction (0422); mandatory.	n/a
Original Trace Number	Systems Trace Audit Number from field 11 of the chargeback transaction (0422); mandatory.	Systems Trace Audit Number from field 11 of the original 0200 or 0220 transaction; mandatory.
Original Transmission Date and Time	Transmission Date and Time from field 7 of the chargeback transaction (0422); mandatory.	Transmission Date and Time from field 7 of the original 0200 or 0220 transaction; mandatory.
Unformatted Text	n/a	Contents depend upon the message reason code. Explanatory text is mandatory when the message reason code is: • 2481 • 2485 • 2486 • 2495 Table 10–7 identifies the explanatory text requirements for transactions with the message reason codes above. Explanatory text is optional when the message reason code is: • 2482 • 2491

Table 10–7 shows the information that must be provided in the Unformatted Text subfield of Field 125—Supporting Information.

Table 10–7: Requirements for Explanatory Text in Field 125

Message Reason Code	Text Requirements
2481	• Systems Trace Audit Number from the adjustment request • Transmission Date and Time from the adjustment request
2485	• Systems Trace Audit Number from the merchandise credit • Transmission Date and Time from the merchandise credit
2486	Supporting text
2498	Free text, clear explanation of the processing error
2495	"Missing required data" or "missing documentation"

Processing specifications for Interlink representment transactions, as specified in the Interlink operating regulations, are summarized in Table 10–8.

Table 10–8: Processing Specifications for Representment Transactions (1 of 2)

Representment Reason	Usage	Time Frame	Documentation or Information Required	Message Reason Code (in Field 63.3)
Adjustment already issued	When the adjustment has already been issued by the acquirer.	The acquirer must re-present within 15 calendar days of receipt of the chargeback.	No documentation required. The message must contain the transmission date and time, and trace number of the adjustment transaction.	2481

Table 10–8: Processing Specifications for Representment Transactions (2 of 2)

Representment Reason	Usage	Time Frame	Documentation or Information Required	Message Reason Code (in Field 63.3)
Invalid chargeback	When the chargeback transaction took place as requested by the cardholder and was without error.	The acquirer must re-present within 15 calendar days of receipt of the chargeback.	The terminal log must show the transmission date and time, trace number, merchant name and location, and transaction amount. The acquirer must have a legible Interlink paper sales draft, if applicable.	2482
Merchandise credit already issued	When a merchandise credit has already been issued.	The acquirer must re-present within 15 calendar days of receipt of the chargeback.	The message must contain the transmission date and time, and trace number of the merchandise credit transaction.	2485
Invalid merchandise credit chargeback	When the merchant member finds no transaction record based on the transaction date supplied in the chargeback transaction for credit not received without receipt.	The acquirer must re-present within 15 calendar days of receipt of the chargeback.	No documentation required.	2486
Missort	When the chargeback is for a transaction that was not processed by the acquirer.	The acquirer must re-present within 15 calendar days of receipt of the chargeback.	No documentation required.	2491
Required data not received	When required data, documentation, or information is not received from the issuer.	The acquirer must re-present within 15 calendar days of receipt of the chargeback.	No documentation required. The message must contain the transmission date and time, the trace number of the chargeback, and an explanation.	2495

Administrative Messages

Acquirers use administrative messages to:

- Request general information or transaction-specific information to properly process representments.
- Initiate administrative messages to alert an issuer that requested information has been sent, as in the case of retrieval requests.
- Respond to issuer requests for additional information about chargebacks.

IMPORTANT

The acquirer's staff must initiate administrative messages and respond to administrative messages from issuers.

Interlink Paper Sales Drafts

Interlink paper sales drafts are paper-based transactions initiated at the POS because the merchant's terminal or the cardholder's card was not functioning properly.

If an acquirer has decided to support Interlink paper sales drafts, the acquirer must convert Interlink paper sales drafts into electronic transactions. This process involves manually entering paper sales draft transactions into the acquirer's exception processing system for electronic forwarding to SMS.

These transactions are considered to be original purchases because there are no previous electronic transactions. They do not contain magnetic stripe data or Personal Identification Number (PIN) information.

IMPORTANT

Only acquirers can initiate paper sales drafts, because these transactions move funds between acquirers and issuers. Merchants are not permitted to enter paper sales drafts. Acquirers typically use their exception processing systems to resubmit Interlink paper sales draft transactions that may be declined for nonsufficient funds or because daily activity limits are exceeded.

Time frames for processing these transactions are outlined in the Interlink operating regulations. For more information on data elements required within the transaction messages, refer to the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications.*

Exception Processing Design Considerations

Designing an exception processing system presents several special considerations:

Storing and Retrieving Original Transaction Data—Adjustments, chargebacks, and representments must be processed electronically in V.I.P. System message formats and require data from the original transaction.

- Information can be saved in report format and manually retrieved and key-entered.
- Members can create an electronic history file that stores original transaction data for settled financial transactions and program the exception processing system to automatically pull the required information when the exception item is processed.
- Members can elect to use the BackOffice Adjustment System (BOAS).

Ensuring Correct Information in Fields With Variable Data Input Codes—For example, Field 63.3—Message Reason Code, is used to indicate the type of chargeback being initiated. A system might be developed to provide variable text information based on the message reason code in the transaction.

Complying With Processing Sequences and Time Frames— Transactions must be processed within certain time frames.

EXAMPLE

An adjustment must be processed within 45 calendar days following the date of the original transaction. Therefore, acquirers can design their systems to prevent processing an adjustment after 45 days. SMS rejects any transaction processed beyond the allowable time frame.

Exception transactions that can be initiated only under certain conditions are not processed unless the conditions are met. For example, a representment cannot be processed unless a chargeback has been initiated. Acquirers can design their systems to ensure that a chargeback is received before initiating a representment.

Member-to-Visa Connection Options 11

Interlink participation requires that members process all Interlink transactions in full financial mode through SMS.

A Visa member can be connected to VisaNet's Single Message System (SMS) only, to the BASE I and BASE II dual-message systems only, or to all three, depending on the requirements of the product mix offered by the member. SMS supports all products in full financial mode. The BASE I and BASE II dual-message systems support all products except Interlink.

Visa Access Point (VAP) Options

A member connects to VisaNet through a VAP, which is a Visa-owned, PC-based system located in the member's processing center. A VAP can connect the member to the BASE I and BASE II dual-message systems, SMS, or all three.

VAPs can support both online interchange and batch processing. Members can transfer report and data files using a VAP's BASE II or Direct Access Service (DAS) application. The VAP must be running VAP Software Release 10.23 or higher. The VAP Release 10.23 documentation is for PS/2 architecture. The VAP Release 11 documentation is for PCI and ISA architecture.

Online interchange is always processed by the V.I.P. component of the VAP, which handles BASE I and SMS online traffic. The V.I.P. component can reside on the same VAP as the BASE II or DAS components, or on a separate VAP. The following descriptions assume the V.I.P. component is on the same VAP as the BASE II or DAS components.

VAP Files

VisaNet delivers report and data files to the VAP with the files' records inside "envelopes" called Transaction Code (TC) records. TC record formats are described in the files chapter of the *V.I.P. System SingleConnect Service SMS Interlink Technical Specifications.*

If the member is not ready to receive files at its host as soon as the VAP receives them from VisaNet, the VAP stores the files for later delivery to the member.

VAP File Types

SingleConnect members can receive all data and report records at the VAP in a single, undifferentiated file (File Type UNDIF). Alternatively, the Customized Delivery feature allows members to request individual files for some types of data and reports. Routing table files are not available through Customized Delivery and are delivered as shown in Table 11–1.

Table 11–1: VAP File Types

File Name and Description	File Type (VAP Pullkey)	TC Records Used For Data Records or Printlines
Undifferentiated • Interlink Routing Table • Interlink Routing Table Report • All data and report records not selected for Customized Delivery	UNDIF	Routing Table: TC 33 TC type shown below for distinct data and report types
Raw Data Machine-readable raw data for reconciliation	DBRAW	TC 33
DS Reports SMS reports	DBRPT	TC 45
VSS Reports—Machine Readable	SETLM	TC 46
VSS Reports—Print-Ready	SETLP	TC 47
VSS Reports—Both Machine-Readable & Print-Ready	SETLR	TC 46 TC 47

File Transfer Connectivity Between VAP and Host

Members can choose from among the following connectivity options to transfer files between their VAP and host:

- TCP/IP FTP file delivery over Token Ring or Ethernet

  Visa provides the member with procedures for TCP/IP FTP delivery. No additional design is required for receipt of a file on the host.

- Visa File Transfer Program (VFTP)

  Visa provides this program to members running MVS on IBM or IBM-compatible hosts. Members choosing to transfer files using VFTP may select one of the following protocol connectivity options:

  – SNA LU0 using Token Ring

  – SNA LU0 Synchronous Data Link Control (SDLC)

  – 2780 Point-to-Point protocol on a Binary Synchronous Communications (BSC)

  – 3270 BSC Multipoint

  – Coax

- Member-designed file transfer

  Visa provides specifications for member use in developing a VAP-to-host file transfer application.

- Tape or Diskette

  The BASE II and DAS File Processors on the VAP enable delivery of files to tape or diskette. Various labeling options are available for tape transfer.

- Remote Job Entry (RJE)

  Visa supports the 2780/3780 point-to-point protocol on a Binary Synchronous Communication (BSC) for RJE file transfer. This connectivity option is available only to members using the DAS delivery service.

For more information on options for transferring report and data files from the VAP to a member's host, see the *VisaNet Access Point Interface Specifications: BASE II & Other File Processing.*

Member Host Processing of Files Received from VAP

Members may want to write software programs to print or manipulate data transferred into their hosts.

VAP With V.I.P. and BASE II Components

A VAP configured for V.I.P. and BASE II supports online and batch processing for all Visa products. This VAP allows members to:

- Send and receive online authorizations and full financial transactions through the V.I.P. component.
- Send and receive clearing and exception transactions for products, BINs, or card ranges not converted to SMS processing through the BASE II component.
- Receive end-of-day reports and files from SMS and the BASE II Clearing and Settlement System through the BASE II component

The BASE II component sends files to, and receives files from, a Visa-supplied Edit Package. The Edit Package resides in the member's host. It is designed to:

- Ensure the integrity of the batch clearing and exception transactions that the member sends to the BASE II System.
- Perform final processing of transactions that BASE II sends to the member, including the transactions (TC records) that make up end-of-day reports and files.

For more information on the functions of the Edit Package, see the *BASE II Clearing & Settlement System Edit Package Operations Guide* or the *BASE II PC Edit Package User's Guide.*

VAP With V.I.P. and DAS Components

A VAP configured for V.I.P. and DAS can be used by SingleConnect members. This VAP configuration allows members to:

- Send and receive online authorizations and full financial transactions through the V.I.P. component.
- Receive end-of-day report and data files from SMS and the BASE II Clearing and Settlement System through the DAS component

DAS handles report files differently from data files. DAS strips all data files of hash bytes but not header and trailer records. At the member's option, DAS delivers the DS Reports file (DBRPT) as 133-byte printlines or as data records with embedded printlines. The member always receives the International and National Net Settlement Report file (SETLR) as 133-byte printlines. This report file does not have header and trailer records.

For more information on DAS, contact your Visa representative.

VAP Options for New SingleConnect POS Endpoints

A new participant in V.I.P. SingleConnect POS Service processing can choose the BASE II or DAS component to connect to VisaNet for file delivery. Typically, DAS is selected based on its simpler operating requirements (the Edit Package is not necessary), especially if the member's future plans are to support all other Visa products in a single-message environment.

SMS Functions To Be Supported

There are three basic functions that V.I.P. SingleConnect Service participants must support:

- Online transaction processing
- Settlement and reconciliation
- Exception handling

Each of these functions is discussed in the following sections.

Online Transaction Processing

This section identifies the message format and delivery requirements for online transaction processing.

Online Message Format

All message types, both financial and nonfinancial, are supported by the V.I.P. message format. The V.I.P. format is required for online financial processing.

The BASE I message format supports nonfinancial message types only. This format is used by many issuers for their current VisaNet interfaces.

A member can choose to continue to use the BASE I format for existing Visa products and add the V.I.P. format for online financial processing. In this case, two separate ports are required on the VAP, one for each message format.

Instead of supporting two formats, all processing can be performed through a single V.I.P. interface on the VAP. In this case, BASE I transactions must be converted from the BASE I format to the V.I.P. format.

Online Transaction Delivery

Real-time messages (in both V.I.P. and BASE I formats) are always delivered through the V.I.P. System component of the member's VAP. The V.I.P. System component can be either on the same VAP as the BASE II or DAS components, or on a separate VAP.

Settlement and Reconciliation Report Delivery Options

At the end of each day, members' VAPs receive settlement and reconciliation reports from VisaNet.

A member may want to receive its SingleConnect reports or raw data, or both, through its BASE II interface, along with any other batch data being delivered from the BASE II System for other Visa products supported by the member. A Visa-supplied Edit Package is used to extract and print the reports. The BASE II reports use a different port than that used for online transaction delivery.

Members connected exclusively to SMS can receive their reports and raw data through DAS, without using a Visa Edit Package in their host systems. Batch report and file delivery is always performed on a separate port than that used for online transaction processing.

Exception Handling

A member must decide how to set up its exception handling interface. Exception handling is a process in which staff members:

- Accumulate exceptions during the day.
- Conduct inquiries.
- Follow up on correspondence.
- Submit adjustment transactions to the interchange system.

Members typically establish a workstation platform for this purpose. The workstation can be a stand-alone system, connected to the member's host, or both.

Once a member is ready to transmit the accumulated exception items, the exception handling system is connected to SMS. This connection is often through a dial-up line, and transactions are transmitted conversationally.

BackOffice Adjustment System (BOAS)

Members that do not already have an exception handling system for SingleConnect transactions can choose to use Visa's stand-alone BackOffice Adjustment System (BOAS) connected to SMS through the VAP.

For a member that uses BOAS, the origination and receipt of all Visa POS and Visa Electron exception items are handled on a platform separate from the member's host system.

BOAS is available from Visa as stand-alone software that runs on the member's IBM or IBM-compatible personal computer.

Because the BOAS software is offered by and maintained by Visa, and is available for immediate shipment to a member, BOAS often saves the time and expense involved in building and maintaining an automated exception system.

BOAS communicates with VisaNet through a dedicated port on the member's VAP. To send or receive exception transactions, the member must be signed on to VisaNet.

Acquirers can initiate the following transactions from a BOAS terminal:

- Adjustments
- Representments
- Fee collections and funds disbursements
- Free text messages

Acquirers can receive the following transactions at a BOAS terminal:

- Chargebacks
- Chargeback reversals
- Fee collections and funds disbursements (issuer-generated)
- Free text messages (issuer-generated)

Issuers can initiate the following transactions from a BOAS terminal:

- Chargebacks
- Chargeback reversals
- Fee collections and funds disbursements
- File maintenance
- Free text messages

Issuers can receive the following transactions at a BOAS terminal:

- Adjustments
- Representments
- Fee collections and funds disbursements (acquirer-generated)
- Free text messages (acquirer-generated)

For more information on BOAS, see the list of BOAS documents in the "For More Information" section of the About This Manual chapter at the front of this manual.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

Z