Welcome to

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

This revised manual, which describes Single Message System (SMS) POS processing for Visa and Visa Electron, 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.

In companion volumes, the SingleConnect technical specifications for Visa POS and Visa Electron describe 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 POS (Visa & Visa Electron) Processing Specifications

SingleConnect Service

V.I.P. System

Effective: 31 March 2001

Printed on recycled paper.

Contents

Chapter 1 • Service Overview

Chapter 4 • Message Types and Flows

Chapter 5 • Multicurrency Support

Chapter 6 • Stand-In and Card Verification Value Processing

Chapter 10 • Member-to-Visa Connection Options

Chapter 11 • Considerations for Issuers

Appendix A • Visa Secure Electronic Commerce

Index

Figures

Tables

About This Manual

The *V.I.P. System SingleConnect Service SMS POS (Visa & Visa Electron) Processing Specifications* manual provides general information about the SingleConnect Service for Visa POS and Visa Electron. 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 POS (Visa & Visa Electron) 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 Visa POS and Visa Electron processing.

Audience

The processing specifications in this manual are intended for technical and systems professionals responsible for implementing the SingleConnect POS Service for Visa POS and Visa Electron 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 Visa POS and Visa Electron features and services.

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

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

Chapter 4, Message Types and Flows—Provides descriptions and message flow diagrams for Visa POS and Visa Electron 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 Visa POS and Visa Electron participants. Additional risk services are also described.

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

Chapter 8, Routing—Contains information about Visa POS and Visa Electron 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, Member-to-Visa Connection Options—Contains information on connectivity requirements and options.

Chapter 11, Considerations for Issuers—Provides information on processing deferred clearing transactions and repeat transactions.

Appendix A, Visa Secure Electronic Commerce—Contains a description of VSEC processing, related messages, and the coding for key fields.

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.

V.I.P. System 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: 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 0838-01

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 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 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 POS (Visa & Visa Electron) 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 POS (Visa & Visa Electron) Processing Specifications*:

V.I.P. SingleConnect Service POS—Visa & Electron Reference Guide, Processing Specifications

V.I.P. System User's Manual Volume 3A, Debit Processing

V.I.P. System Technical Reference Volume 3B, Debit Settlement and Reports

Technical Letters

The *V.I.P. System SingleConnect POS (Visa & Visa Electron) 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. Copies beginning May 2000 include Visa Smart Debit and Visa Smart Credit.

Visa Latin America and Caribbean Regional Operating Regulations

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

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 POS (Visa and 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 Interlink Reference Guide, Processing Specifications—This manual contains information about the SingleConnect Interlink Service and its support of Interlink transactions. It includes information about message types, processing considerations, security responsibilities, related services, and connection options.

V.I.P. System SingleConnect Service Interlink Reference Guide, 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 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 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

DCAF Service

For more information about DCAF, refer to:

Deferred Clearing Advice File (DCAF) Member Implementation Guide

Deferred Clearing Advice File (DCAF) Service Technical Specifications

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

Fraud Reporting System 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

VisaNet Copy Request and Fulfillment Service (VCRFS)

For information about VisaNet Copy Request and Fulfillment Service (VCRFS), refer to:

VCRFS Copy Request Manager User's Guide

VCRFS Fax Gateway User's Guide

VCRFS Processing Guide

VisaNet Image Gateway Image Interface Technical Specifications

VisaNet Image Gateway User's Guide

Visa Smart Debit and Visa Smart Credit (VSDC) Documentation

Visa provides the following manuals to describe the functions and features of the Visa Smart Debit and Visa Smart Credit chip technology program.

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

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

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

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

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

V.I.P. System Reports

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):

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

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.

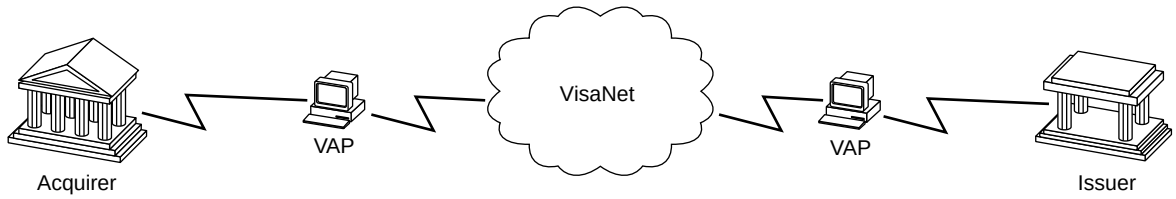
NOTE: *Some readers may have seen online financial processing referred to as single-message processing; Visa's preferred terminology distinguishes between the Single Message System and the SingleConnect Service (which is processed through the Single Message System).*

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



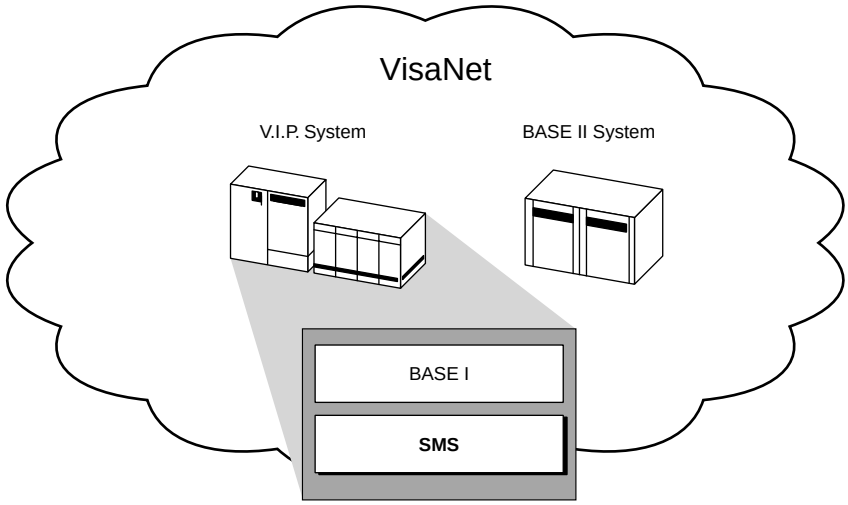
VisaNet Systems

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.
- The BASE II System, which supports dual-message clearing functions.

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 products and use SMS processing for debit products.

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

A bridge between BASE I and SMS makes it possible for BASE I and SingleConnect users to communicate with each other.

For information about SMS gateways to outside networks, refer to the Gateway Services chapter of *V.I.P. System Services*.

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

The V.I.P. System is the primary online transaction switching and processing system for all transactions that enter VisaNet. The V.I.P. System provides 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 (CMI) and Other Access Methods

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:

- Visa.
- Visa Electron.
- Interlink and Visa Interlink. For information about Interlink processing, refer to the *V.I.P. System SingleConnect Service SMS Interlink Processing Specifications*.
- Some non-Visa products.

SMS supports SingleConnect ATM transactions for:

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

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

The V.I.P. SingleConnect Service can provide faster clearing and settlement, 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.

This manual discusses only those aspects of BASE I that relate to transactions involving SMS. Refer to the About This Manual chapter for a complete list of BASE I manuals.

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.

VisaNet Settlement Service (VSS)

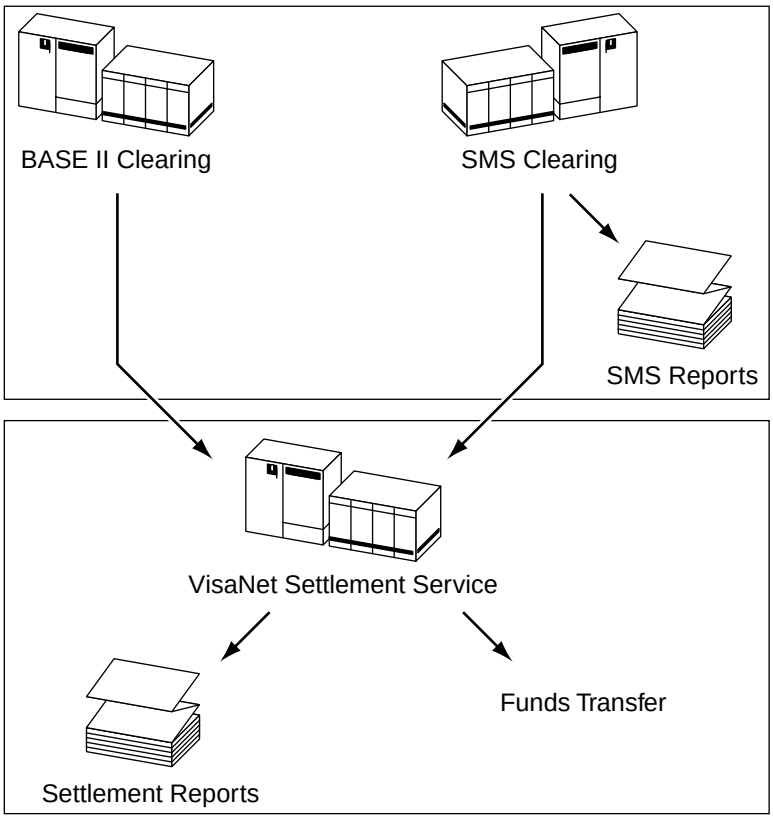
VSS consolidates settlement functions for the Single Message System (SMS) and the BASE II System in one service. Members and processors receive SMS and BASE II settlement information in a standardized set of reports. VSS provides flexibility in defining financial relationships, selecting reports and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



SMS POS Processing Summary

The following is a brief description of how a typical online financial SMS POS 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.

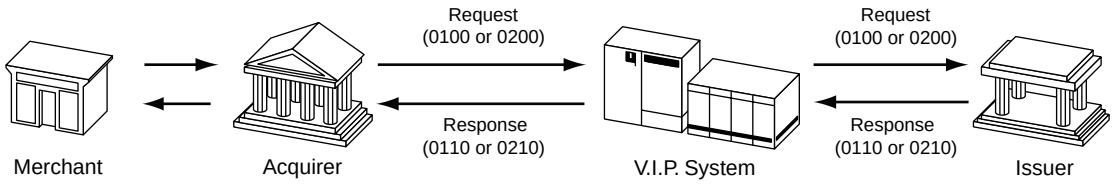
SMS POS Online Transaction Flow

Figure 1–4 illustrates how an 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.
   - A merchant manually enters the card number into a terminal.

   PINs are conditional in Visa and Visa Electron transactions. (PINs are required in Interlink and ATM transactions).
2. The merchant's acquirer takes the information and creates an 0100 authorization 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 authorization 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 (POS) 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



For Visa and Visa Electron deferred clearing purchases, acquirers also can use 0220 advices to submit purchase transactions. For details, refer to Chapter 4, Message Types and Flows.

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) can be 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 more 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:

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

IMPORTANT

SMS does not have the STIP functionality that BASE I does. Consequently, the processing of credit transactions through SMS is at the region's discretion.

Visa, Visa Electron, and Interlink 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.

SingleConnect POS Service for Acquirers

SMS allows SingleConnect POS 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:
  - Visa and Visa Electron POS acquirers can use online deferred clearing processing.
  - 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.

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 conditional for Visa and Visa Electron but required for Interlink. 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.

SingleConnect POS Service for Issuers

Participating issuers can process Visa, Visa Electron, and Interlink 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 and receive online deferred clearing transactions through the V.I.P. System at a later time.

For batch deferred clearing transactions from traditional BASE I/BASE II Visa and Visa Electron acquirers or online deferred clearing transactions from SingleConnect acquirers, issuers receive the authorization message at the time of purchase and the clearing message later. (See Chapter 4, Message Types and Flows, and Chapter 11, Considerations for Issuers, for more information about processing deferred clearing transactions.)

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 all Visa-branded products.

The main function of issuers' systems is to accurately respond, 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 POS transactions for Visa or Visa Electron, or both. (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 through SingleConnect.

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.

In addition to the following discussion, refer to Chapter 8, Routing, for more information about the routing services.

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.

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.

Split Routing

Two Split Routing services are available to SingleConnect POS issuers:

- Split Routing (ATM/POS)—This service enables issuers to separate message traffic into ATM and POS transaction routes.
- Split Routing (PIN/No-PIN)—This service enables issuers to separate POS message traffic requiring PINs from message traffic not requiring PINs (called *No-PIN transactions*).

Authorization Services

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

Address Verification Service (AVS)

AVS is an online Visa service that enables merchants to reduce fraud losses by verifying cardholders' billing addresses. The service currently applies to U.S. domestic and U.K. domestic transactions only. V.I.P. removes any address information from other international transactions.

Effective 15 May 2001, the new International Address Verification Service will be extended to all regions.

For more information, contact your Visa representative.

Card Verification Value (CVV) Service

The 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 authorization 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 (CVV2) Service

The CVV2 Service is a card verification tool designed to reduce fraud losses on transactions when the card is not present.

Issuers must imprint a 3-digit security number (the CVV2) on the back of all new or reissued Visa cards, in accordance with *Visa International Operating Regulations*. Members can use the CVV2 number to validate that a genuine Visa card is present during a transaction. The CVV2 is calculated using a secure cryptographic process and a key known only to the issuer and Visa.

Participating merchants manually enter the CVV2 numeric value for validation by the V.I.P. System, the issuer, or both. V.I.P., the issuer, or both verify the CVV2 and return the CVV2 result code to the merchant.

All Visa cards (including emergency replacement cards) must carry the CVV2 security number.

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

Automatic Cardholder Database (Auto-CDB) Update

The Auto-CDB Update service enables SingleConnect issuers to update the SMS Exception File through authorization response messages.

Auto-CDB helps issuers prevent losses from problem accounts and improves the accuracy of cardholder information available to VisaNet for stand-in (STIP) processing.

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

International Automated Referral Service (IARS)

IARS enables acquirers to reach any Visa issuer promptly whenever the issuer needs more information from the acquirer before making an authorization decision. IARS guarantees a response to every referral call, even when the issuer is unavailable. This service helps reduce Visa sales losses caused by authorization delays.

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

PIN Verification Service (PVS)

PVS provides full-time or stand-in verification of personal identification numbers (PINs) used for ATM transactions, Interlink 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 details about this service, refer to Chapter 7, Security.

Dynamic Key Exchange (DKE) Service

The 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.

Risk Services

Visa offers the following tools to issuers and acquirers that enable them to minimize their exposure to fraud. Most of the risk services are optional.

Fraud Reporting System (FRS)

FRS helps members report, track, and analyze fraudulent transactions. FRS consolidates fraud information, helping members detect fraud patterns and reduce losses.

Members are required to electronically report confirmed fraud transactions on all Visa cards. Acquirers and issuers must comply with the fraud reporting rules as defined in the Visa operating regulations.

The SMS Online Fraud Reporting option, available through V.I.P., allows single-message users to report fraud using SMS advice messages. This option is not available for Interlink.

SMS connected endpoints can also receive fraud reporting confirmation messages through the online interface.

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

Cardholder Risk Identification Service (CRIS)

CRIS is a Risk Management service that provides authorization scoring and reporting to alert issuers of potentially fraudulent activity on Visa accounts. The service uses neural networks and risk-scoring models to analyze individual authorizations worldwide through VisaNet.

The neural networks recognize specific fraudulent patterns and discriminate between low- and high-risk authorizations. Additionally, Visa continually updates the neural network risk-scoring models to account for changing fraud patterns for each region.

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

Additional Services

This section includes additional services available to SMS 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, CRIS, Fraud, BASE II, funds transfer, fee collections/disbursements, and so on.

Members can use the DCAF service to retrieve original BASE II draft transactions in a file instead of individually from the online advice queue. All other types of advices from BASE II endpoints (that is, those advices that are not original BASE II draft transactions) must be recovered through the online connection—not DCAF.

Members can also elect to have Visa hold advices from BASE II endpoints until a certain time of day to manage the volume of advices efficiently. This option is explained in the following section, "Flexible Times for Online Delivery of Advices from BASE II Endpoints."

For more information about DCAF, refer to the "Deferred Clearing Advice File (DCAF) Service" section later in this chapter.

For more information about the SMS Advice Retrieval Service, refer to the advice recovery sections of Chapter 4, Message Types and Flows, and Chapter 6, Stand-In and Card Verification Value Processing.

Flexible Times for Online Delivery of Advices from BASE II Endpoints

To manage the volume of advices from BASE II endpoints, members can specify times for retrieving these advices from online queues. (Also see "DCAF Service" in the next subsection, which explains how SMS issuers can receive original BASE II clearing transactions in bulk files.)

DCAF Service processing options relate specifically to original BASE II deferred clearing transactions received through file delivery. The flexible timing options described in this section, however, apply to all advices received online from acquirer or issuer BASE II endpoints.

With implementation of the flexible timing options, advices from BASE II endpoints are available to SMS issuers shortly after clearing BASE II. To facilitate different members' processing needs, SMS issuers can specify one of the following options at the BIN or processor level:

- Define a specific delivery time for advices from BASE II endpoints.
- Retrieve advices from BASE II endpoints as soon as they become available to V.I.P., currently as early as noon Pacific standard time (PST).
- Retrieve advices from BASE II endpoints at the standard system default time.

For more information about these options, contact your Visa representative.

Deferred Clearing Advice File (DCAF) Service

The DCAF service allows members processing in a single-message environment to receive original BASE II deferred clearing advices in bulk file deliveries. (Also see "Flexible Times for Online Delivery of Advices from BASE II Endpoints," which explains how members can specify times for retrieving BASE II advices from online queues.)

BASE II deferred clearing advices originate from dual-message acquirers that do not generate online clearing messages. Without the DCAF service, Single Message System (SMS) members receive deferred clearing advices online, one advice per station at a time. In certain cases, capacity problems can occur due to the volume of deferred clearing advices.

To alleviate capacity and resource contention problems, the DCAF service allows issuers to receive deferred clearing advices in bulk files. Bulk file delivery uses network lines separate from online station lines. This reduces issuers' online host and network capacity requirements and helps members manage receipt of large volumes of advices.

For more information about DCAF, contact your Visa representative or refer to:

- The *Deferred Clearing Advice File (DCAF) Member Implementation Guide (Document ID 2904-01).*
- The *Deferred Clearing Advice File (DCAF) Service Technical Specifications (Document ID 2901-02).*

Visa Secure Electronic Commerce (VSEC) Consumer Payment Service

VSEC technology protects card-not-present transactions occurring over the Internet and other networks. VSEC authorization requests involve digital certificates and SET Secure Electronic Transaction™ technology. (SET™ is a joint Visa-MasterCard development.)

VSEC transactions are treated as retail transactions and must be authorized online using a zero floor limit. STIP is invoked only when the issuer is unavailable.

For more information, see Appendix A, Visa Secure Electronic Commerce.

Visa Smart Debit and Visa Smart Credit (VSDC)

VSDC is a chip-based solution that allows members to combine the functionality of Visa's debit and credit products with the strategic flexibility of chip technology. VSDC offers a suite of optional risk control features that can be tailored to the transaction type, market segment or to the individual cardholder. These features are available only through chip technology.

VSDC provides issuers with the ability to securely modify chip controls without card reissuance. Visa provides members with a phased approach to incorporate chip technology while building the chip infrastructure. VSDC offers enhanced control and security over magnetic stripe technology, and worldwide interoperability through the use of the *EMV Integrated Circuit Card Specifications for Payment Systems*.

For a full description of VSDC, refer to the *Visa Smart Debit and Visa Smart Credit Service Description*, which provides a high-level description of the features and benefits of a VSDC program. To plan a VSDC program and migration strategy, refer to *Visa Smart Debit and Credit Planning Guide*.

VisaNet Copy Request and Fulfillment Service (VCRFS)

VCRFS facilitates the process of requesting and delivering copies of sales drafts between members and merchants. In addition, VCRFS permits Visa to perform compliance monitoring and dispute mediation, while reducing costs and increasing customer satisfaction. The goal of this service is to fully automate all copy request fulfillments based on member needs and cost effectiveness.

For a description of VCRFS field coding and message formats, refer to the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications*.

For more information about VCRFS, refer to the *VCRFS Processing Guide*.

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.

International Outgoing Interchange (IOI) Fees

IOI fees are assessed by Visa to the sender of a transaction when a transaction is acquired outside of the card issuer's country. IOI fees may vary by Visa region. The fees are usually calculated as a percent of the transaction amount.

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 to both 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 POS Transactions 2

This chapter identifies the SingleConnect transactions supported for Visa and Visa Electron in the POS environment, gives a brief description of each transaction type, and explains how SingleConnect participants maintain message integrity for all transactions.

Transaction Types

Table 2–1 lists the transactions allowed and supported for Visa and Visa Electron in the POS environment. For comparison, Interlink transactions are also included in the table, but not in the transaction descriptions that follow it.

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

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

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

Transaction Type	Message Type	Visa	Visa Electron	Interlink
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	✔	✔	
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	✔	✔	✔

Cardholder Transactions

The following transactions are supported for Visa and Visa Electron in the POS environment.

Authorization—V.I.P. SingleConnect Service acquirers use an authorization transaction message when the final transaction amount is not known at the time of purchase. This transaction is available for Visa and Visa Electron.

Manual Cash Disbursement—This transaction is used for manual cash disbursements (also called manual cash), and is available for Visa and Visa Electron.

Purchase—The purchase transaction is the basic POS transaction used for Visa and Visa Electron processing. The flow of a purchase transaction is described in the "SMS POS Online Transaction Flow" section of Chapter 1, Service Overview.

Variations of the purchase transaction include:

- Purchase with cashback.
- Quasi-cash.
- Key-entered purchase.

Purchase with Cashback—Cashback is a variation of the purchase transaction that permits the cardholder to get cash in addition to goods or services. For Visa Electron, the availability of this transaction is governed by regional operating regulations. Purchase with cashback is not available for Visa.

Quasi-Cash—Quasi-cash is a variation of the purchase transaction, used for the purchase of items that are directly convertible to cash, such as gaming chips and money orders. It is available for Visa and Visa Electron.

Key-Entered Purchase—This transaction is a variation of the purchase transaction, used only for Visa and Visa Electron transactions when the magnetic stripe on the card is not readable.

Deferred Clearing Purchase Transaction—This transaction is used by such merchants as hotels and car rental agencies when the full purchase amount is not known at the time of transaction authorization. This transaction, used only by Visa and Visa Electron acquirers, involves an authorization request followed by a deferred clearing advice message.

Merchandise Return—A merchandise return transaction enables merchants to credit the account of a Visa or Visa Electron cardholder who returns merchandise.

System-Generated Transactions

The following transactions are supported for Visa and Visa Electron.

Reversals

A reversal transaction, which is system-generated, can be initiated by an acquirer's host system or by V.I.P.

Issuers and acquirers must match reversals to the corresponding 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.

Acquirer-Initiated Reversals—POS acquirers and merchants use reversals to reverse approved authorizations or financial transactions that were not completed due to system malfunctions or because the transactions timed out. Financial transactions are:

- Manual cash disbursements.
- Purchases (all types).
- Merchandise returns.

Deferred clearing purchase transactions can be reversed.

POS reversals can be used by:

- 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.-Initiated Reversals—V.I.P. initiates 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 for Visa and Visa Electron are used to correct errors that occur at the point of transaction or in a participant's system:

- Adjustment
- Chargeback

- Chargeback reversal
- 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.

In addition, Visa and Visa Electron issuers must be able to create chargeback reversals, and Visa and Visa Electron acquirers must be able to receive chargeback reversals. Each of these types of exception transactions is discussed in this section.

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). Adjustment transactions are supported for Visa and Visa Electron.

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

Chargeback transactions are supported for Visa and Visa Electron.

Chargeback Reversal—Visa or Visa Electron issuers can create a chargeback reversal to cancel a prior chargeback transaction that was sent in error.

Representment—Acquirers can create a representment transaction message to debit a cardholder's account when the validity of a chargeback can be disproved. Representments are supported for Visa and Visa Electron.

Fee-Related Transactions

There are two types of fee-related transactions for Visa and Visa Electron, both of which have financial value:

- Fee collections—These transactions are used to collect miscellaneous fees.
- Funds disbursements—These transactions are used to remit miscellaneous fees.

These transactions, which are available for both Visa and Visa Electron, do not require authorization and cannot be declined.

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 Visa and Visa Electron 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, Exception File, or Address Verification File. An update advice is also provided to Automatic Cardholder Database Update (Auto-CDB) Service participants.
- File Inquiry—This transaction is used to review the issuer's entries on the PIN Verification File, Exception File, or Address Verification 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 Chapter 5, Message Formats, of the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications.*

For details about online file maintenance messages, see Chapter 4, Message Types and Flows, and the message formats chapter of the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications.*

Administrative Transactions

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

SingleConnect administrative messages consist of:

- Copy Requests and Confirmations—These transactions are used to request copies of previously submitted transactions and to confirm their receipt. These transactions are available for Visa and Visa Electron.
- VCRFS Transactions (Visa and Visa Electron Only)—These transactions include the following message types:
  - Copy Request—The issuer submits an administrative message for copy request processing.
  - Copy Fulfillment—The acquirer sends an electronic image of the requested item along with additional requested data.
  - Nonfulfillment—The acquirer uses this response to notify the issuer that the copy being requested will not be sent. The message includes the reason for the nonfulfillment.
  - Mail Fulfillment—An acquirer or merchant sends this response to inform the issuer that the requested copy is being sent through the mail. Except for the reason code, the mail fulfillment and nonfulfillment messages are identical
  - Dispute Request—SMS issuers participating in VCRFS can submit dispute request advices after receiving copy fulfillments. The dispute request advices must contain the reason codes indicating why the issuers are disputing the acquirers' fulfillment of the copy requests. Dispute request advices are routed to the Visa Mediation Service for resolution.
  - Dispute Ruling—The Visa Mediation Service makes rulings on items disputed by issuers. Once the Visa Mediation Service rules on a disputed item, a dispute ruling is sent to the issuer. If the ruling is in favor of the issuer, a dispute ruling also is sent to the acquirer.
- 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, not codes, they can be routed to a printer, for manual evaluation, or documented on a report. These messages are available for Visa and Visa Electron.
- Funds transfer—These messages are used to send the day's final funds transfer totals after completion of settlement and reconciliation.
- CRIS Alerts—These messages notify subscribing issuers of cardholder accounts with levels of risk equal to or above subscriber-defined thresholds.
- Online Fraud Reporting—These messages are used to report fraud transactions that VisaNet passes to the Fraud Reporting System.

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

Network Management Transactions

SingleConnect 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.

VSDC Transactions

To see how POS transactions are processed by the Visa Smart Debit and Visa Smart Credit (VSDC) product, refer to the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications.* For a discussion of VSDC transactions, refer to sources listed in Chapter 1, Service Overview.

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, only certain transactions are allowed, and within a given transaction, only certain system transactions are allowed.

Visa and Visa Electron transaction sets consist of the following:

- Manual cash disbursement
- Purchase
- Deferred clearing purchase with online authorization
- Merchandise return

The following tables, beginning with Table 2–2 and ending with Table 2–5, show the valid Visa and Visa Electron 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, chargeback reversal, and representment.

Note that 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.

Table 2–2: Manual Cash Disbursement Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Chargeback Reversal	Representment
Cash Disbursement	✔	✔	✔	✔	✔
Adjustment	✔		✔	✔	✔

Table 2–3: Purchase Transaction Set

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

[1] Includes purchase with cashback (Visa Electron only), quasi-cash, and key-entered purchase.

Table 2–4: Deferred Clearing Purchase with Online Authorization Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Chargeback Reversal	Representment
Authorization	✔	✔			
Deferred Clearing Purchase	✔	✔	✔	✔	✔
Adjustment	✔		✔	✔	✔

NOTE: *Values in the retrieval reference number and system trace audit number from the authorization may not match the values in the deferred clearing message.*

Table 2–5: Merchandise Return Transaction Set

Allowable Transactions	Request	Reversal	Chargeback	Chargeback Reversal	Representment
Merchandise Return	✔		✔	✔	✔
Adjustment	✔		✔	✔	✔

Message Integrity

Maintaining message integrity is a basic requirement of the V.I.P. SingleConnect Service processing. Message integrity assures V.I.P. SingleConnect Service 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 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. VisaNet enforces these rules by comparing an incoming message with previous messages containing the same key data elements. In general, VisaNet rejects any message that is out of context or out of sequence.

VisaNet 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, an authorization 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.

All transactions within a transaction set must contain the same transaction amount except for chargebacks, representments, and adjustments. 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, and Transmission Date and Time) as a prior message. V.I.P. processes duplicates as follows:

- If processing of the original request was completed (a response was sent), V.I.P. 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, V.I.P. does not involve STIP or the issuer. V.I.P. logs the request and response.
- If processing of the original request is still in progress, VisaNet logs the duplicate, then discards it. (VisaNet assumes that the original will be completed; therefore the duplicate is not needed.)

Repeat messages, used by BASE I acquirers when a transaction times out, may not be submitted by SingleConnect acquirers. Issuers should see Chapter 11, Considerations for Issuers, for more information on repeats.

Service Participation Requirements 3

This chapter summarizes the required and optional functionality for acquirers and issuers that participate in the V.I.P. SingleConnect Service for Visa and Visa Electron in a POS environment. 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 Visa and Visa Electron programs.

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

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 Visa and Visa Electron transactions. Alternatively, members can designate third-party processors to complete the certification process and process Visa and Visa Electron transactions on their behalf.

All Visa or Visa Electron 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.

- Participate in the Visa online Multicurrency Service, and be able to receive the multicurrency fields in online messages, and raw data files if the raw data option is selected (optional for members in the U.S. region).
- Use VisaNet Access Point (VAP) Software Release 10.2 or higher.
- Complete technical certification. The certification process covers all relevant message types, raw data, and reports. VisaNet Test System pre-certification scripts are available from your Visa representative.
- Comply with all applicable Visa operating regulations.
- Log all transactions, whether approved or declined, in order to reconcile to Visa settlement positions.
- Support exception processing, as specified later in this chapter.
- If Personal Identification Numbers (PINs) are supported, processing requirements must meet the standards specified in Chapter 7, Security.
- Support fee collections and funds disbursements
- Participate in the VisaNet Settlement Service (VSS).
- Participate in the Card Verification Value (CVV) Service. Nonparticipants are liable for counterfeit magnetic stripe transactions.
- Participate in the Fraud Reporting System (FRS) and be able to create 9620 advice messages. For more information, refer to Chapter 4, Message Types and Flows.

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

Transactions that must be supported by all Visa and Visa Electron acquirers are specified in Table 3–1.

Table 3–1: Required Acquirer Transactions

Transaction Type	Visa	Visa Electron
Manual Cash Disbursement	✔	✔
Purchase	✔	✔
Reversal	✔	✔
Adjustment	✔	✔
Chargeback	✔	✔
Chargeback Reversal	✔	✔
Representment	✔	✔
Fee-Related Transactions	✔	✔
Administrative Transactions (can be submitted using BOAS)	✔	✔
Free Text Message	✔	✔
Copy Request/Confirmation	✔	✔
Funds Transfer	✔	✔
CRIS Alerts	✔	✔
Network Management Transactions	✔	✔
Responses 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.

Additionally, Visa and Visa Electron acquirers must meet the following service requirements:

- To process an online financial transaction (0200), the final purchase amount must be known at the time of purchase. (See the "Deferred Clearing Processing" section of this chapter for requirements for handling purchases for which the final amount is not known at the time of the purchase.)
- All transactions must be authorized online by the issuer or authorized by stand-in processing (STIP).
- In a card-present environment, transactions must contain the full unaltered data content of the card's magnetic stripe. If the magnetic stripe cannot be read, Visa card transactions can be key-entered at the merchant's and acquirer's risk. Visa Electron card transactions cannot be key-entered.
- In a card-not-present environment (as in the case of mail and telephone orders), Visa card transactions can be key-entered. Visa Electron card transactions cannot be key-entered.
- Acquirers must reverse back to the issuers any transactions not completed as requested for any of the following reasons:
  - No response is received from VisaNet.
  - A late response is received from VisaNet.
  - The transaction is cancelled at the point of sale.
  - The transaction response cannot be successfully delivered to the terminal.
- Acquirers must process system-generated reversals online.

Deferred Clearing Processing

Visa and Visa Electron acquirers can optionally process online deferred clearing transactions (0220s) in addition to online financial transactions. To process deferred clearing transactions, acquirers must meet the following service requirements:

- To process a purchase transaction for which the amount is not known at the beginning of the transaction, participating Visa and Visa Electron acquirers must use a deferred clearing purchase transaction. An online authorization message is followed by an online deferred clearing message. The amount in the authorization can differ from the amount in the clearing message.
- Acquirers must reverse back to the issuers any transactions not completed as requested for any of the following reasons:
  - No response is received from VisaNet.
  - A late response is received from VisaNet.
  - The transaction is cancelled at the point of sale.
  - The transaction response cannot be successfully delivered to the terminal.
- Deferred clearing transactions must be routed and processed using standard Visa and Visa Electron operating regulations.
- Participating acquirers must support authorization reversal transactions.
- The deferred clearing advice must identify whether the card was magstripe read or key-entered. Magstripe data must be included on the advice when applicable.

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.

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

Visa Secure Electronic Commerce (VSEC) Processing

VSEC processing is required for Visa and Visa Electron card-not-present transactions occurring over the Internet and other networks. For details, refer to Appendix A, Visa Secure Electronic Commerce.

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.

In addition, acquirers must support copy requests and confirmations. Acquirers can meet this requirement by using the VisaNet Copy Request and Fulfillment Service (VCRFS).

Acquirer Options

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

Optional transactions for SMS acquirers are listed in Table 3–2.

Table 3–2: Optional SMS Acquirer Transactions

Transaction Type	Visa	Visa Electron
Authorization	✔	✔
Quasi-Cash	✔	✔
Key-Entered Purchase	✔	✔
Deferred Clearing Purchase	✔	✔
Merchandise Return	✔	✔
Reconciliation Transactions	✔	✔
File Maintenance Transactions	✔	✔
VCRFS transactions	✔	✔

In addition, SMS acquirers can use or support the following services and capabilities listed in Table 3–3.

Table 3–3: Acquirer Options (1 of 2)

Options	References
Currency Precision Service	Chapter 5, Multicurrency Support
Card Verification Value 2 (CVV2)	Chapter 6, Stand-In and Card Verification Value Processing
Online fraud reporting	Chapter 4, Message Types and Flows
Dynamic Key Exchange	Chapter 7, Security

Table 3–3: Acquirer Options (2 of 2)

Options	References
Visa Routing Table	Chapter 8, Routing
Choice of settlement options	Chapter 9, Settlement and Reconciliation
Visa BackOffice Adjustment System (BOAS)	Chapter 10, Member-to-Visa Connection Options
Choice of one or more VAP options	Chapter 10, Member-to-Visa Connection Options
Choice of report delivery options	Chapter 10, Member-to-Visa Connection Options
Choice of detailed reports	*The VisaNet Settlement Service (VSS) User's Guide*
Receipt of raw data files	Appendix A, Files, of the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications*
Visa Smart Debit and Visa Smart Credit (VSDC)	*Visa Smart Debit and Credit Planning Guide* and the *Visa Smart Debit and Credit Member Implementation Guide*

Issuer Requirements

Issuer systems are required to respond to Visa and Visa Electron messages sent from VisaNet. This 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 Visa or Visa Electron cards in accordance with all applicable Visa operating regulations.
- Support PIN processing requirements as defined in Chapter 7, Security.

Transaction Processing

Participating issuers must support the full set of transactions initiated by SMS acquirers and VisaNet. Requirements by card type are specified in Table 3–4.

Table 3–4: Required Visa and Visa Electron Issuer Transactions (1 of 2)

Transaction Type	Visa	Visa Electron
Cardholder Transactions		
Authorization	✔	✔
Manual Cash Disbursement	✔	✔
Purchase	✔	✔
Quasi-Cash	✔	✔
Key-Entered Purchase	✔	
Deferred Clearing Purchase	✔	✔
Merchandise Return	✔	✔
System-Generated Transactions		
Reversal	✔	✔
Exception Transactions (requirement can be met through BOAS)		
Adjustment	✔	✔

Table 3–4: Required Visa and Visa Electron Issuer Transactions (2 of 2)

Transaction Type	Visa	Visa Electron
Chargeback	✔	✔
Chargeback Reversal	✔	✔
Representment	✔	✔
Fee-Related Transactions		
Acquirer-Generated Fee Collection/Funds Disbursement	✔	✔
Issuer-Generated Fee Collection/ Funds Disbursement	✔	✔
Reconciliation Transactions	✔	✔
Online File Maintenance	✔	✔
Administrative Transactions		
Free Text Message	✔	✔
Copy Request/Confirmation (requirement can be met through VCRFS)	✔	✔
Funds Transfer	✔	✔
CRIS Alerts	✔	✔
Online Fraud Reporting	✔	✔
Network Management Transactions	✔	✔
Responses to each of these transactions	✔	

Visa and Visa Electron issuers receive each Visa and Visa Electron transaction as either an online financial or deferred clearing transaction, according to the manner in which the transaction originates from the merchant or the acquirer:

- Transactions originated by merchants or acquirers as online financial transactions are routed, received, and processed by issuers as full financial, immediately postable transactions, following Visa or Visa Electron online financial message operating regulations.
- Transactions originated by merchants or acquirers as deferred clearing transactions may be received by issuers in two parts:
  - Authorization request
  - Online deferred clearing advice

Required Capabilities for Issuers

The following capabilities are required for issuers.

PIN Verification

Each SingleConnect POS issuer must provide PIN verification capability or subscribe to the Visa PIN Verification Service (PVS) if they process transactions with PINs.

Visa and Visa Electron issuers can use the Extended Service Codes in magnetic stripe data that are designated for Visa and Visa Electron cards to communicate their card acceptance policies, including those for PIN verification.

Issuers that support Visa Smart Debit and Visa Smart Credit (VSDC) may elect to use Offline PIN for certain transactions and cardholders, as described in the *Visa Smart Debit and Visa Smart Credit Service Description*.

Card Verification Value 2 (CVV2) Service

All Visa cards (including emergency replacement cards) must carry the CVV2 security number.

Exception Processing

Visa and Visa Electron participants must support exception processing. For issuers, this includes the ability to initiate chargebacks and chargeback reversals, and accept adjustments, representments, and administrative messages. Issuers can meet this requirement by using the Visa BackOffice Adjustment System (BOAS).

In addition, Visa and Visa Electron issuers must support the following transactions:

- Copy requests and confirmations (requirement can be met through VCRFS)
- 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 SingleConnect POS issuers are listed in Table 3–5

Table 3–5: Issuer Options (1 of 2)

Options	References
Multicurrency Service: • Issuer markup for currency conversion • Currency Precision Service	Chapter 5, Multicurrency Support
STIP processing: • PIN Verification Service • Exception File Service • Mod-10 Check Digit Verification	Chapter 5, Stand-In, CVV, and CVV2 Processing
Cardholder Risk Identification Service (CRIS) and online CRIS alerts	Chapter 6, Stand-In and Card Verification Value Processing
Card Verification Value 2 (CVV) Service	Chapter 6, Stand-In and Card Verification Value Processing
Online Fraud Reporting	Chapter 4, Message Types and Flows
International Automated Referral Service (IARS)	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	*VisaNet Settlement Service (VSS) User's Guide*
Reconciliation messages	Chapter 4, Message Types and Flows
Visa BackOffice Adjustment System (BOAS)	Chapter 10, Member-to-Visa Connection Options
Choice of one or more VAP options	Chapter 10, Member-to-Visa Connection Options

Table 3–5: Issuer Options (2 of 2)

Options	References
Choice of report delivery options	Chapter 10, Member-to-Visa Connection Options
Choice of detail reports	*VisaNet Settlement Service (VSS) User's Guide*
Receipt of raw data files	Appendix A, Files, of the *V.I.P. SingleConnect Service POS (VISA & VISA Electron) Technical Specifications*
VisaNet Copy Request and Fulfillment Service (VCRFS)	*VCRFS Processing Guide*
Visa Smart Debit and Visa Smart Credit (VSDC)	*Visa Smart Debit and Credit Planning Guide* and the *Visa Smart Debit and Credit Member Implementation Guide*

Message Types and Flows 4

This chapter describes the message flows for Visa and Visa Electron 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
  - 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:
  - Authorization
  - Financial Transactions
  - Reversals
  - Exception Transactions

Standard Processing

This section describes the following transactions processed under standard conditions.

- Cardholder Transactions
  - Purchases and Manual or Cash Disbursements
  - Online Deferred Clearing
  - Merchandise Return
- System-Generated Transactions
  - Reversals
- Exception Transactions
  - Adjustments
  - Chargeback
  - Representment
- Reconciliation Transactions
  - Requested Reconciliation Advices
  - Automatic Reconciliation Advices
- File Maintenance Transactions
  - Online File Maintenance
  - Automatic Cardholder Database Update
- Administrative Transactions
  - Free Text Message
  - Copy Request and Confirmation
  - Funds Transfer Message
  - Online Fraud Reporting
- Network Management Transactions
  - Sign-On and Sign-Off Messages
  - Echo Test Messages
  - Recovery Sign-On and Sign-Off Messages
  - Dynamic Key Exchange

For each transaction illustrated in this chapter, a table appears indicating the support of Visa and Visa Electron cards.

Cardholder Transactions

The following flow diagrams and descriptions illustrate the flows for POS transactions initiated by the cardholder.

Purchases and Manual or Cash Disbursements

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

Visa Electron *cashback* transactions are also included in the flows for this category. 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.

For SingleConnect participants outside the U.K., Field 4—Amount, Transaction must contain the total transaction amount, which is the sum of the purchase amount and the cashback amount. For the U.K., a purchase with cashback transaction differs from a purchase by an amount in Field 61.1—Other Amount, Transaction. Regional operating regulations can apply to cashback transactions.

A manual cash disbursement is a transaction where the cardholder obtains cash in a face-to-face environment. It is valid for both Visa and Visa Electron.

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

A standard purchase or manual cash disbursement transaction is composed of two messages:

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

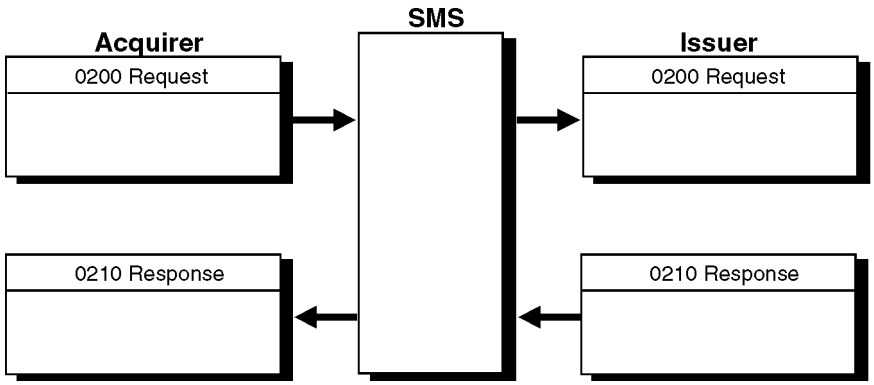
Table 4–1 also identifies the different purchase types.

Table 4–1: SingleConnect POS Service Purchase Types

SMS Product Service	Purchase	Purchase with Cashback	Quasi-Cash	Key-Entered
Visa	✔		✔	✔
Visa Electron	✔	✔	✔	

Figure 4–1 illustrates the standard flow of a purchase or manual cash disbursement transaction.

Figure 4–1: Purchase or Manual Cash Disbursement Transaction Flow



Online Deferred Clearing

An 0220 purchase advice (instead of an 0200 financial request) is used to request a financial transaction when a merchant does not know the final purchase amount at the time a transaction is authorized, as occurs with a hotel bill or car rental fee.

In this instance, the acquirer first sends an 0100 authorization message to verify that the cardholder has an account in good standing and receives an 0110 response from the issuer or SMS stand-in-processing (STIP). Then, when the purchase amount is known at a later time, an 0220 acquirer-generated advice is submitted.

Message processing for 0220 deferred clearing advices proceeds as follows:

1. The acquirer logs the transaction and forwards the 0220 financial request message to SMS.
2. SMS logs the transaction, performs currency conversion if needed, and routes the message to the issuer based on the card number.
3. The issuer logs the transaction and sends an 0230 response message to SMS.
4. SMS logs the message and forwards it to the acquirer. The transaction is settled after the next settlement cutoff. An issuer cannot decline an online deferred clearing transaction but may have chargeback rights.

Both Visa and Visa Electron acquirers can submit deferred clearing transactions. The card need not be present for an online deferred clearing transaction.

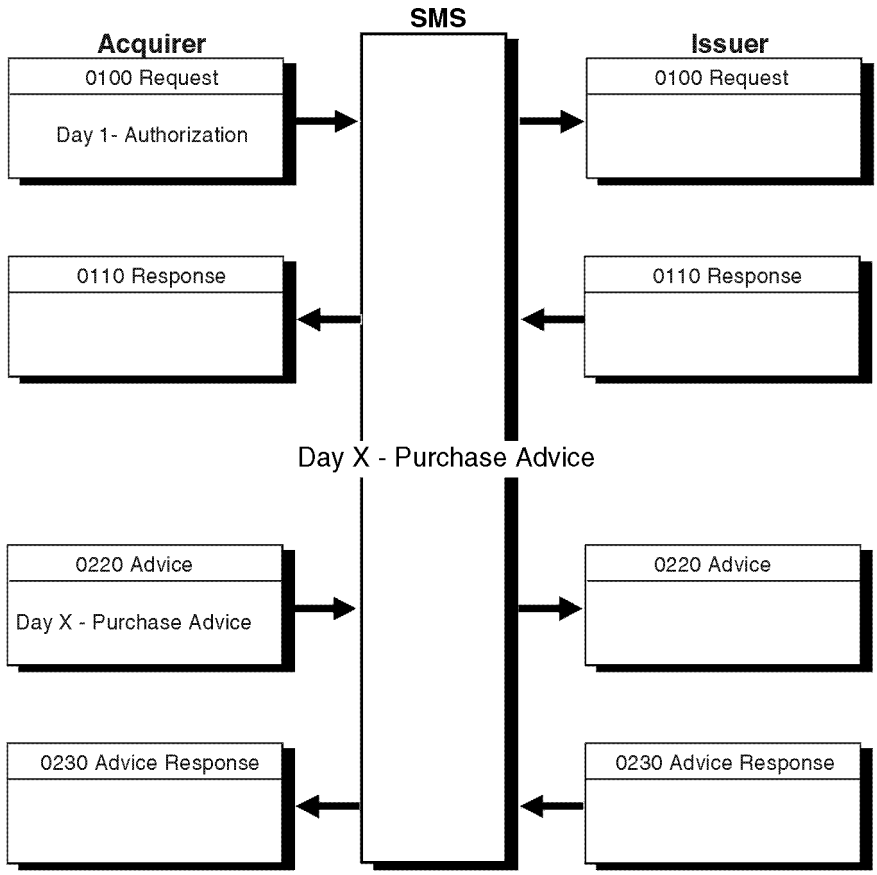
If the acquirer receives a referral response and then obtains a voice approval, the acquirer must send a deferred clearing transaction to SMS with the approval information in Field 39—Response Code.

NOTE: *Online deferred clearing transactions are called acquirer advices in Chapter 5, Message Formats, of the* V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications.

Visa	✔
Visa Electron	✔

Figure 4–2 illustrates an online deferred clearing transaction flow.

Figure 4–2: Online Deferred Clearing Transaction Flow



Merchandise Return

A Visa or Visa Electron merchandise return 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.

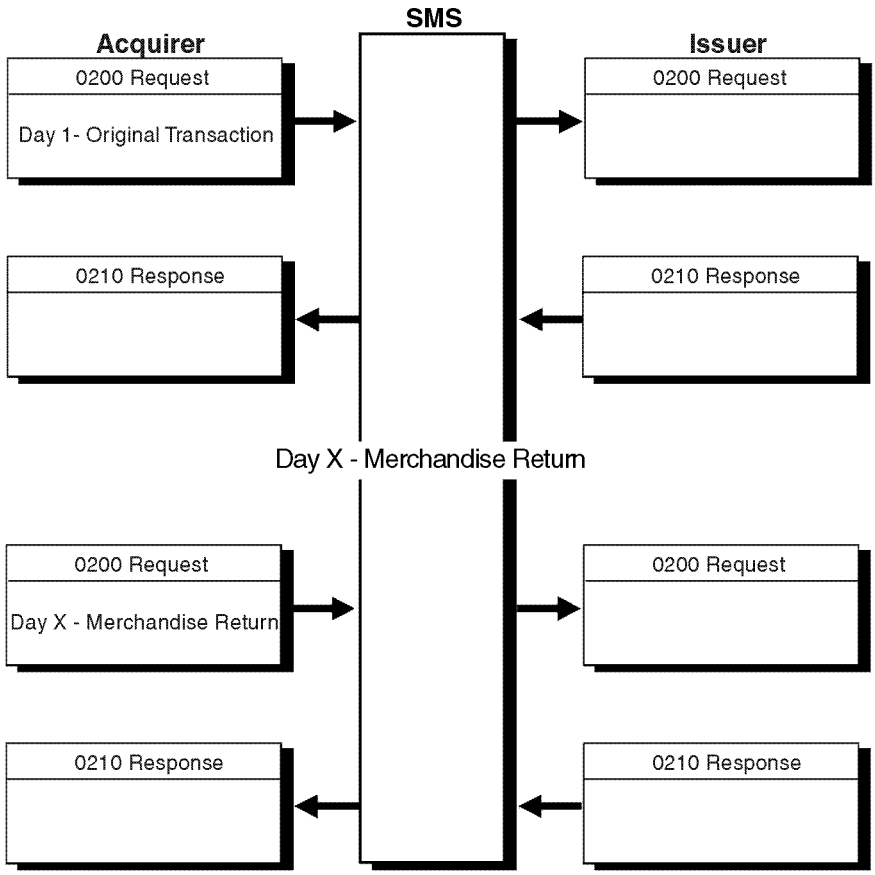
A return is initiated at the point of sale. Use of the same terminal or merchant outlet used for the original purchase is not required.

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 return transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–3: Merchandise Return Transaction Flow



System-Generated Transactions

For the SingleConnect POS Service, system-generated transactions consist of reversals.

Reversals

A reversal cancels an authorization or voids a financial transaction. Either SMS or the acquirer can generate a reversal.

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

  Message reason code 2501 applies to such events.
- 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).
- The acquirer cannot send an approved response to the point of service (message reason code 2503).
- The acquirer receives an approval response from SMS after it has been timed out by its host or the point-of-service device (reason code 2502)
- 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.

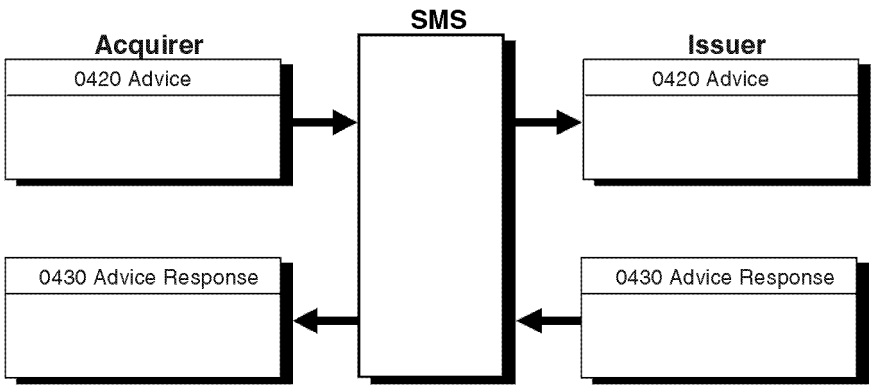
A reversal cannot be declined or reversed. On receipt of a reversal, the issuer should release its hold on funds or reverse the posted transaction from the cardholder's account and from its settlement totals. Reversals are generated to prevent errors in settlement and reconciliation and to enable an 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. Visa recommends the 0420 advices. An 0410 response must be used to respond to an 0400 reversal.

Figure 4–4 illustrates a standard reversal transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–4: Reversal Transaction Flow



Exception Transactions

The following exception transactions are supported for SMS:

- Adjustments
- Chargebacks
- Chargeback Reversals
- Representments

Adjustments

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

There are two types of adjustment transactions:

- Debit adjustments (processing code 02*xxxx*) are used when the cardholder's account was charged less than the actual transaction amount.
- Credit adjustments (processing code 22*xxxx*) 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.

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

Adjustments may be issued on all types of purchase transactions. 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:

- 2007 for POS original adjustments.
- 2009 for POS nonoriginal adjustments.

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.

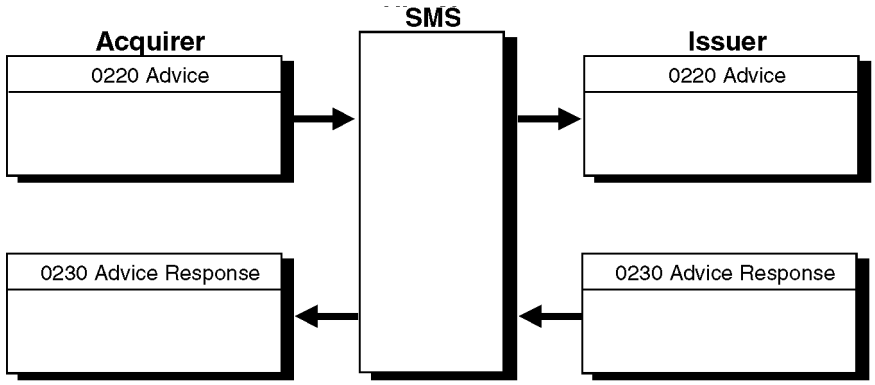
The acquirer cannot reverse an adjustment. Issuers can return invalid debit adjustments or credit adjustments through chargeback transactions.

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 4–5 illustrates a standard (back office) adjustment transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–5: Adjustment Transaction Flow



Chargeback

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. The set number of days varies by the type of chargeback and is within 45 to 180 calendar days of the original transaction. The chargeback amount should be for the original amount and should not include optional issuer fees. The chargeback amount can be for the original amount or can be less than the original amount. 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.

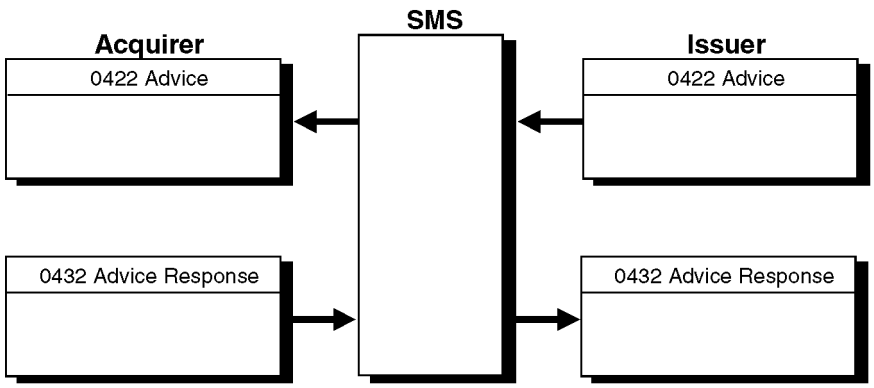
A chargeback can be distinguished from other messages of the same message type by the value of 17 in Field 25—Point of Service Condition Code. Reasons for chargebacks are identified in Field 63.3—Message Reason Code.

Only one chargeback transaction can be processed for a cardholder transaction, although, for select chargeback reasons, issuers can submit a second chargeback after receipt of an acquirer representment. For applicable reason codes, refer to Volume II of the *Visa International Operating Regulations*. For a discussion of the coding requirements for second chargebacks, refer to the field 48, usage 7a description in the *V.I.P. System SingleConnect SMS POS (Visa & Visa Electron) Technical Specifications*.

Figure 4–6 illustrates a chargeback transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–6: Chargeback Transaction Flow



Chargeback Reversal

Chargeback reversals are used by Visa and Visa Electron to cancel chargebacks that were sent in error to acquirers. Chargeback reversals have settlement impact.

An issuer sends an 0422 advice to an acquirer to reverse in full a chargeback that was sent in error. If SMS cannot deliver the advice to the acquirer, it stores the advice for later recovery by the acquirer.

If the chargeback reversal times out at the issuer, the issuer should resubmit the transaction.

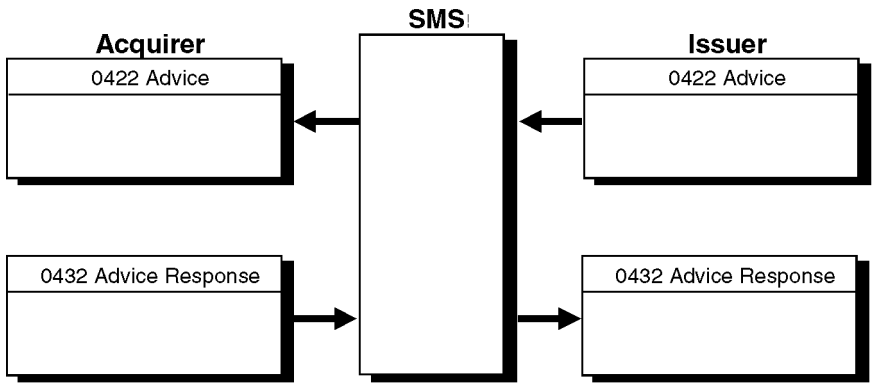
A chargeback reversal must contain the value of 54 in Field 25—Point of Service Condition Code.

Under standard conditions, the acquirer receives an 0422 chargeback reversal advice from the issuer and acknowledges with an 0432 advice response.

Figure 4–7 illustrates a chargeback reversal transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–7: Chargeback Reversal Transaction Flow



Representment

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. Representments must adhere to applicable Visa operating regulations.

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.

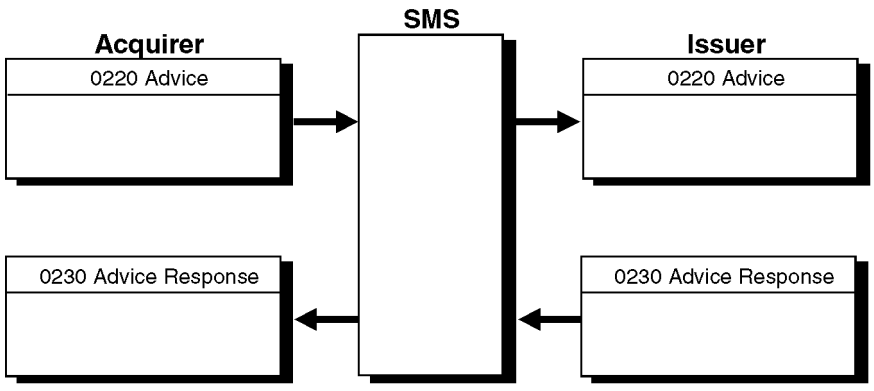
If the representment times out at the acquirer, the acquirer should resend the representment unchanged.

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, and, for Visa and Visa Electron, the code is the same as that of the original chargeback.

Figure 4–8 illustrates a representment transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–8: Representment Transaction Flow



Fee-Related Transactions

A fee-related transaction is a fee collection or funds disbursement transaction. It is used to collect or remit miscellaneous fees such as recovered card rewards. SMS supports fee-related transactions for Visa and Visa Electron.

Acquirers use 0220 advices to send fee-related transactions to issuers. Issuers use 0422 advices to send fee-related transactions to acquirers. These advices contain all the information needed for settlement.

Fee transactions usually do not relate directly to cardholder transactions, and therefore do not result in postings to cardholders' accounts. They are financial in nature, however, and update settlement totals for the sender and receiver. Because fee-related transactions do not require authorization and cannot be declined, they are always processed with advice message types.

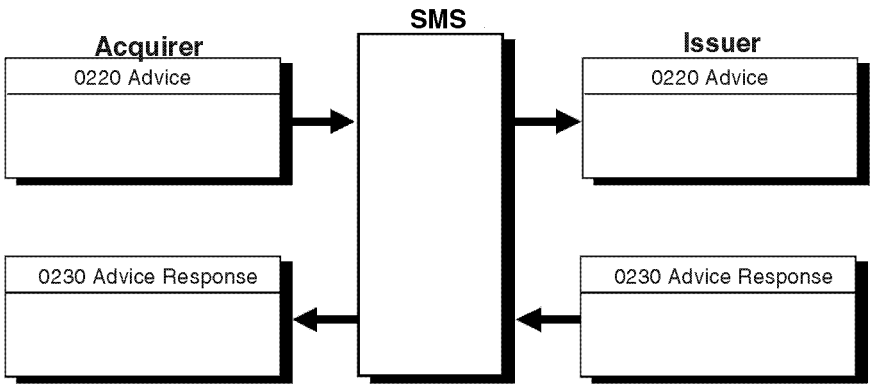
The value in Field 3—Processing Code of a fee collection must be 19*xxxx*. The value in Field 3—Processing Code of a funds disbursement must be 29*xxxx*. These values are used to distinguish fee-related transactions from other transactions with the same message types.

For acquirer-initiated fee-related transactions, under standard conditions, the acquirer sends 0220 fee-related advices to the issuer, and the issuer acknowledges with 0230 advice responses.

Figure 4–9 illustrates an acquirer-initiated fee-related transaction flow.

Visa	✔
Visa Electron	✔

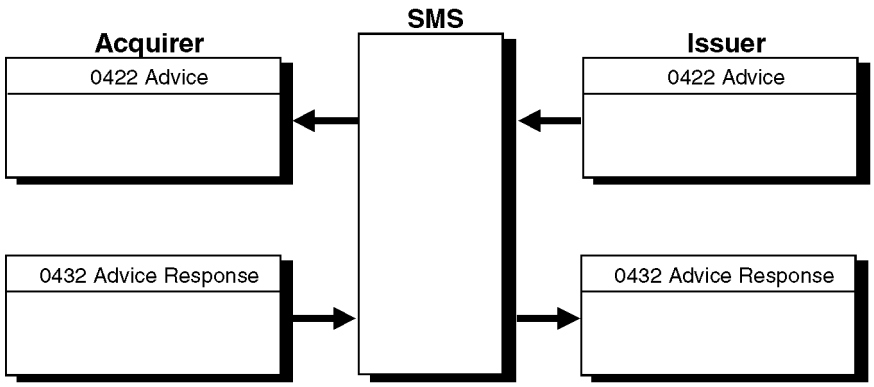
Figure 4–9: Fee-Related Transaction Flow (Acquirer-Initiated)



For issuer-initiated fee-related transactions, under standard conditions, the issuer sends 0422 fee-related advices, and the acquirer acknowledges with 0432 advice responses.

Figure 4–10 illustrates an issuer-initiated fee-related transaction flow.

Figure 4–10: Fee-Related Transaction Flow (Issuer-Initiated)



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 "Automatic Reconciliation Advices" subsection later in this chapter).

Throughout the day, SMS accumulates counts and amounts of transactions that have an effect on 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:

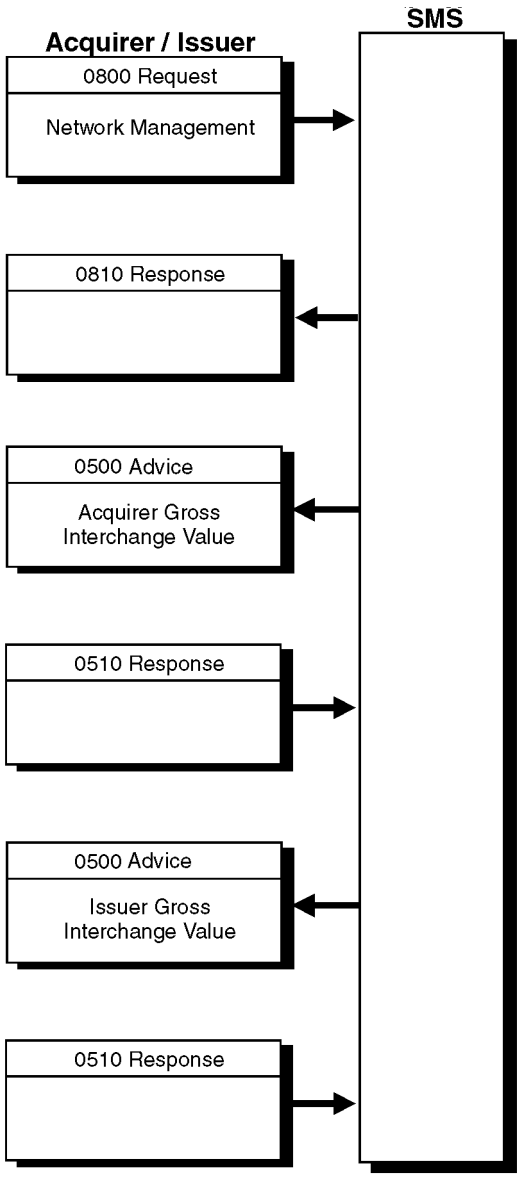
- One contains the Acquirer Gross Interchange Value (acquirer totals plus acquirer STIP totals, if applicable)
- The other contains the Issuer Gross Interchange Value (issuer totals plus acquirer STIP totals, if applicable)

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

Figure 4–11 illustrates the reconciliation transaction process.

Visa	✔
Visa Electron	✔

Figure 4–11: 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

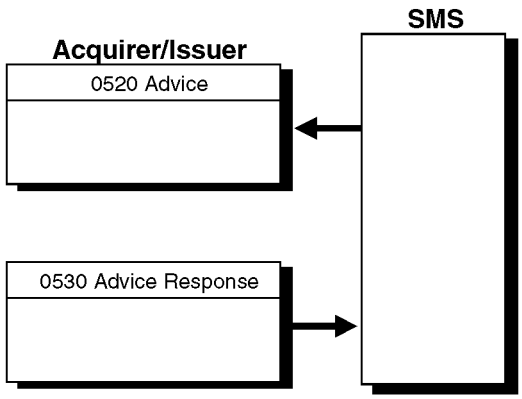
The member acknowledges with an 0530 response message.

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 representative. Members must sign onto advice recovery mode to receive advices.

Figure 4–12 illustrates an automatic reconciliation transaction flow with an 0520 optional advice message.

Visa	✔
Visa Electron	✔

Figure 4–12: Reconciliation Transaction Flow (With an 0520 Optional Advice Message)



File Maintenance Transactions

This section covers two types of file maintenance transactions: online file maintenance and Automatic Cardholder Database (Auto-CDB) Update.

For information on batch file updates, see the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron) 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.

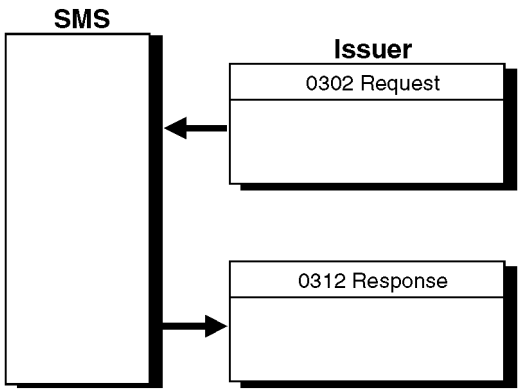
SMS does not create advices for undeliverable 0302 requests.

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 4–13 illustrates a file maintenance transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–13: Online File Maintenance Transaction Flow



Automatic Cardholder Database Update

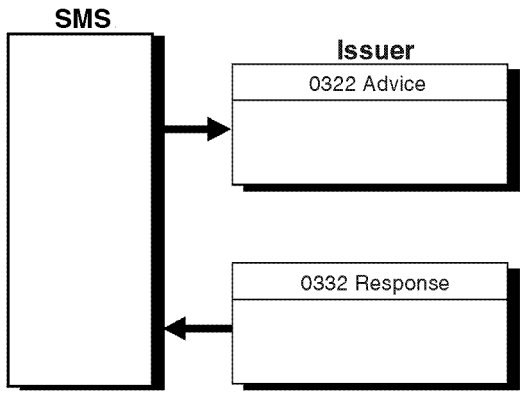
Issuers participating in Automatic Cardholder Database Update (Auto-CDB) receive advices of Exception File additions or updates.

See Chapter 6, Stand-In and Card Verification Value Processing, for more information.

Figure 4–14 illustrates a file maintenance transaction flow for Auto-CDB.

Visa	✔
Visa Electron	✔

Figure 4–14: File Maintenance Transaction Flow for Auto-CDB



Administrative Transactions

There are five types of administrative transactions:

- Free text message
- Copy request and confirmation
- Funds transfer message
- Online fraud reporting

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 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.

Figure 4–15 and Figure 4–16 illustrate free text message transaction flows for acquirer to issuer and issuer to acquirer.

Visa	✔
Visa Electron	✔

Figure 4–15: Free Text Message Transaction Flow (Acquirer to Issuer)

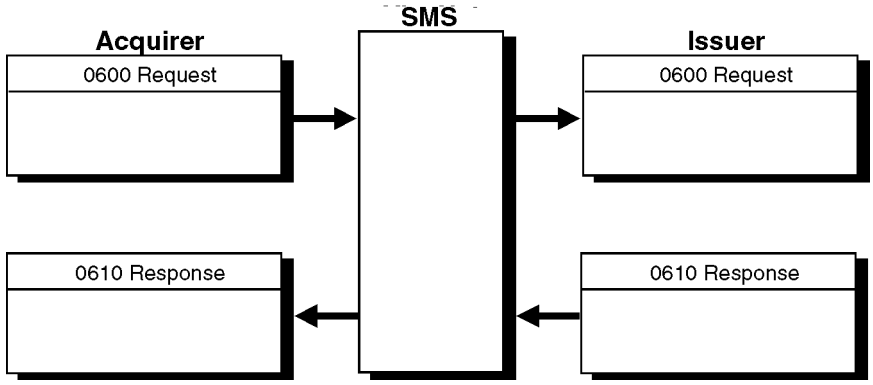
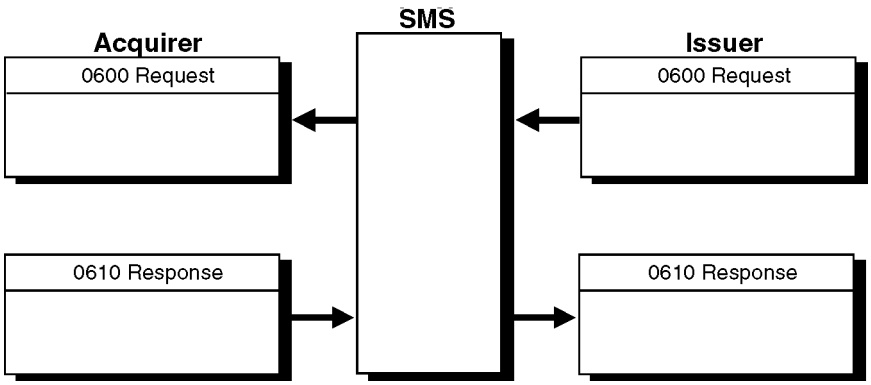


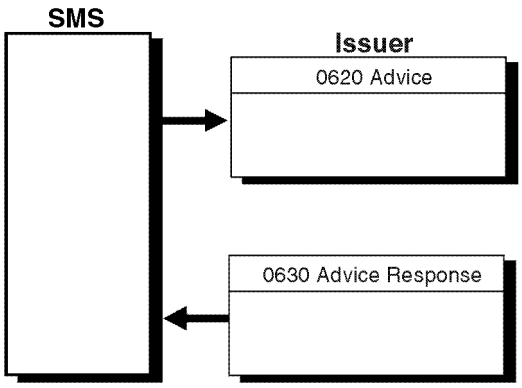
Figure 4–16: Free Text Message Transaction Flow (Issuer to Acquirer)



Cardholder Risk Identification Service (CRIS) participants may receive online alerts through advice recovery mode.

Figure 4–17 illustrates a free text message transaction flow from SMS to an issuer.

Figure 4–17: Free Text Message Transaction Flow—CRIS (SMS to Issuer)



Copy Request and Confirmation

Copy requests and confirmations are administrative messages used to process Visa and Visa Electron requests for documentation. An issuer uses a copy request to request documentation from an acquirer before initiating a chargeback or representment. A confirmation notifies the requesting issuer that the requested documentation has been sent.

Figure 4–18 illustrates a copy request transaction flow, and Figure 4–19 illustrates a copy request confirmation transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–18: Copy Request Transaction Flow (Issuer to Acquirer)

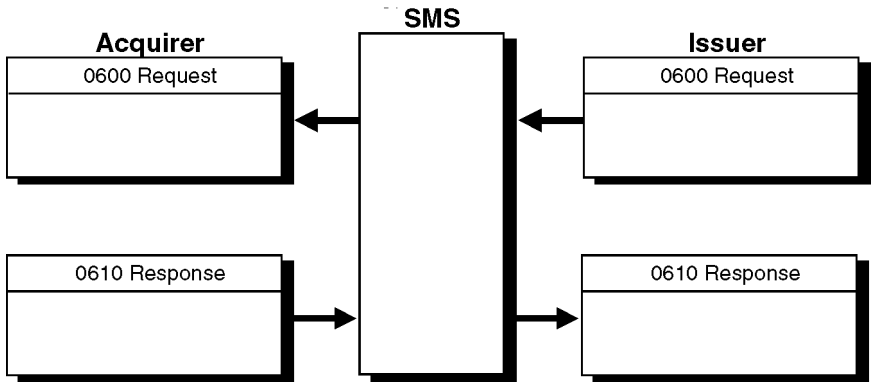
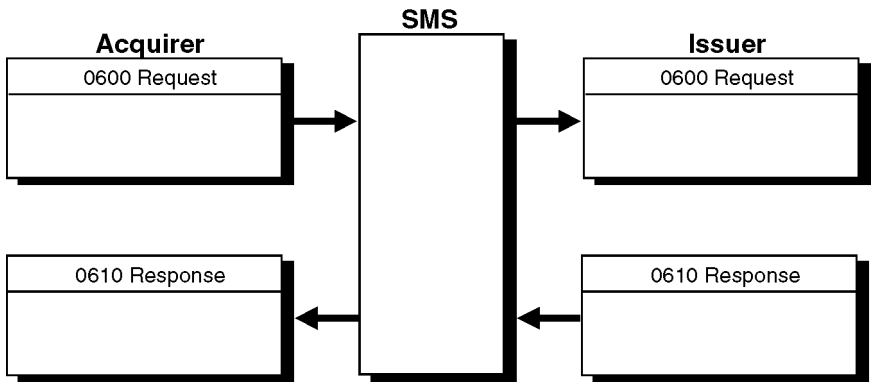


Figure 4–19: Copy Request Confirmation Transaction Flow (Acquirer to Issuer)



If the destination member is not available, SMS accepts the transaction and places an 0620 in the advice queue for the destination member (which could be either an acquirer or an issuer).

Funds Transfer Message

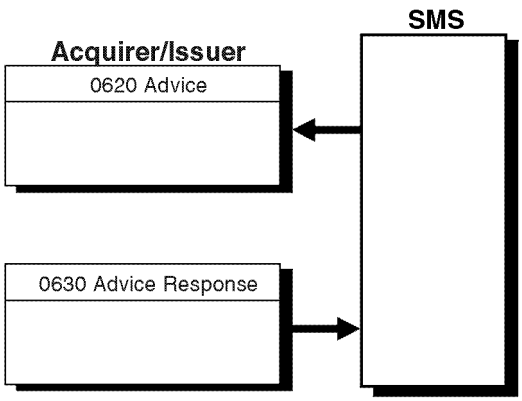
SMS uses 0620 advices to send the day's final funds transfer totals after completion of settlement and reconciliation. Field 48—Funds Transfer Totals (usage 6) contains the settlement totals for the day, including subfields with acquirer, issuer, and net funds transfer totals. The funds transfer message 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 onto advice recovery mode to receive funds transfer messages.

Figure 4–20 illustrates a funds transfer message transaction flow.

Visa	✔
Visa Electron	✔

Funds transfer messages are currently available for SingleConnect members and, in a different format, for members that have migrated to the VisaNet Settlement Service (VSS).

Figure 4–20: Funds Transfer Message Transaction Flow



Online Fraud Reporting

The Online Fraud Reporting capability is optional and allows certified members to report fraud transactions to the Fraud Reporting System (FRS) using online messages. Members also can send fraud notifications through the BackOffice Adjustment System (BOAS).

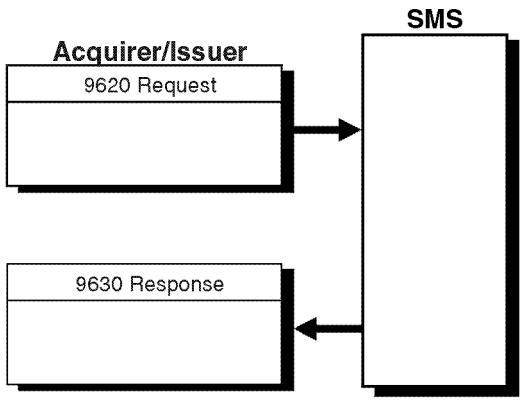
SMS passes the fraud advices to FRS. The fraud transactions are reported to members on the FRS reports. Failure to comply with the fraud reporting rules as defined in the Visa Operating Regulations can result in the loss of chargeback rights and potential fines and penalties.

Issuers and acquirers can use 9620 requests to report confirmed fraud transactions. When SMS receives a 9620 request from the member, it generates a 9630 response.

Figure 4–21 illustrates a fraud reporting message transaction flow.

Visa	✔
Visa Electron	✔

Figure 4–21: Fraud Reporting Message Transaction Flow



Network Management Transactions

All network management transactions are supported for Visa and Visa Electron.

An acquirer or issuer uses 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).

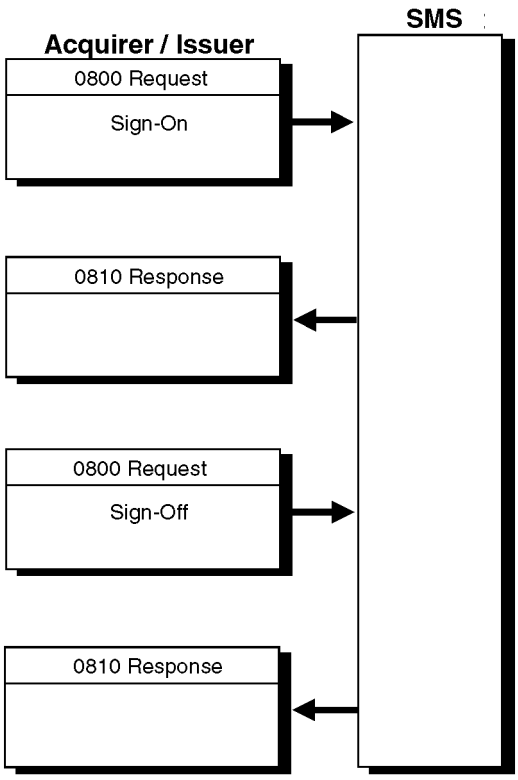
Sign-On and Sign-Off Messages

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

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

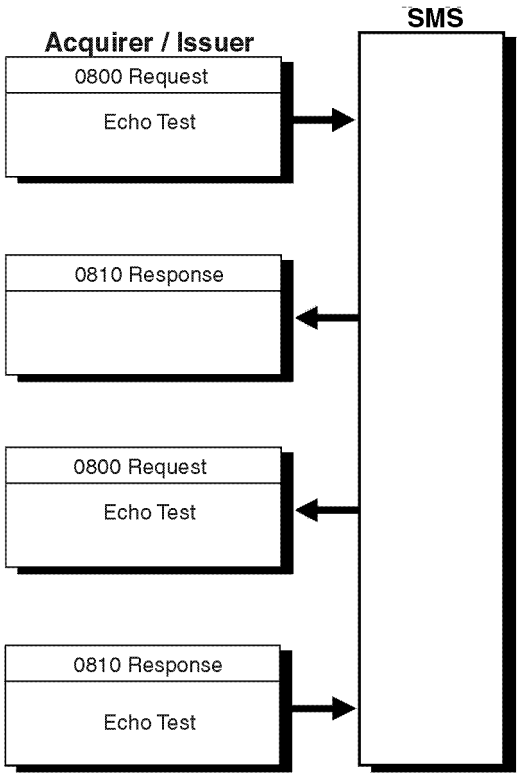


Echo Test Messages

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. Echo tests confirm the availability of the communications link between the acquirer or issuer and SMS.

Figure 4–23 illustrates an echo test message transaction flow.

Figure 4–23: 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.

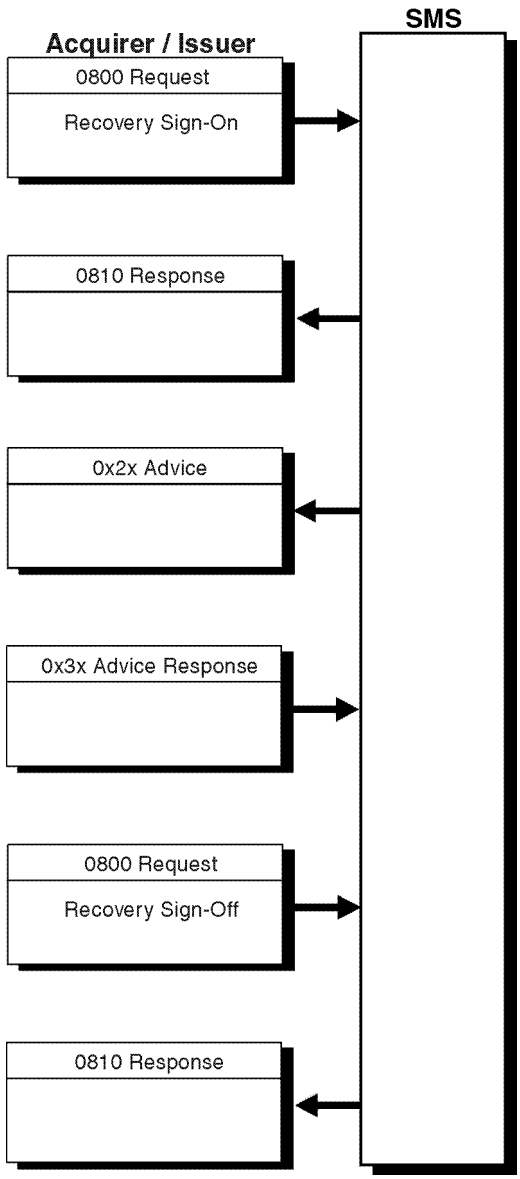
Acquirer and Issuer Recovery

After an issuer or acquirer signs on to advice recovery mode, SMS sends all of the advices (0x2x 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 4–24 illustrates a recovery sign-on and sign-off message transaction flow.

Figure 4–24: Recovery Sign-On and Sign-Off Message Transaction Flow



Dynamic Key Exchange

The Dynamic Key Exchange (DKE) Service is an optional Visa service for SMS members that periodically want to change acquirer and issuer Data Encryption Set (DES) encryption working keys through the exchange of online 0800/0810 messages. For a comprehensive description of the DKE Service, refer to *V.I.P. System Services*.

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.

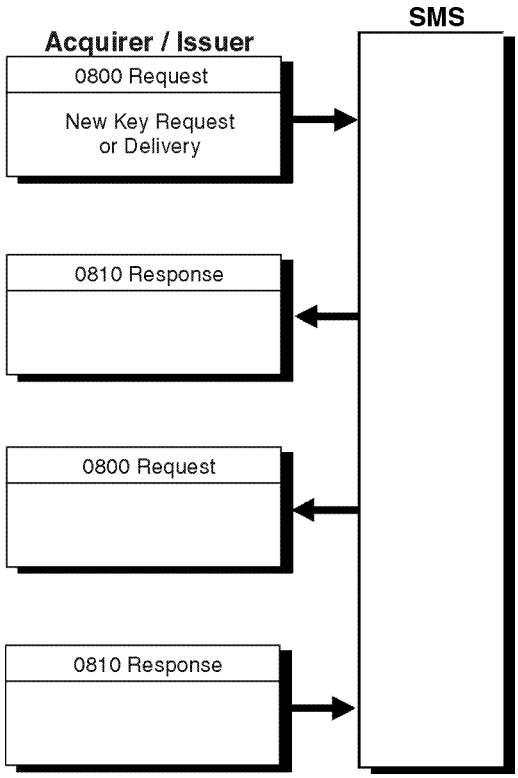
SMS has a 10-second time-out for all dynamic key exchange messages containing new working keys. If the member does not respond within 10 seconds, SMS makes a second delivery attempt. If the member still fails to respond, SMS cancels the key exchange attempt.

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 4–25 illustrates a dynamic key exchange message transaction flow.

Figure 4–25: 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:

- Authorization—Issuer Unavailable
- 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.

Authorization

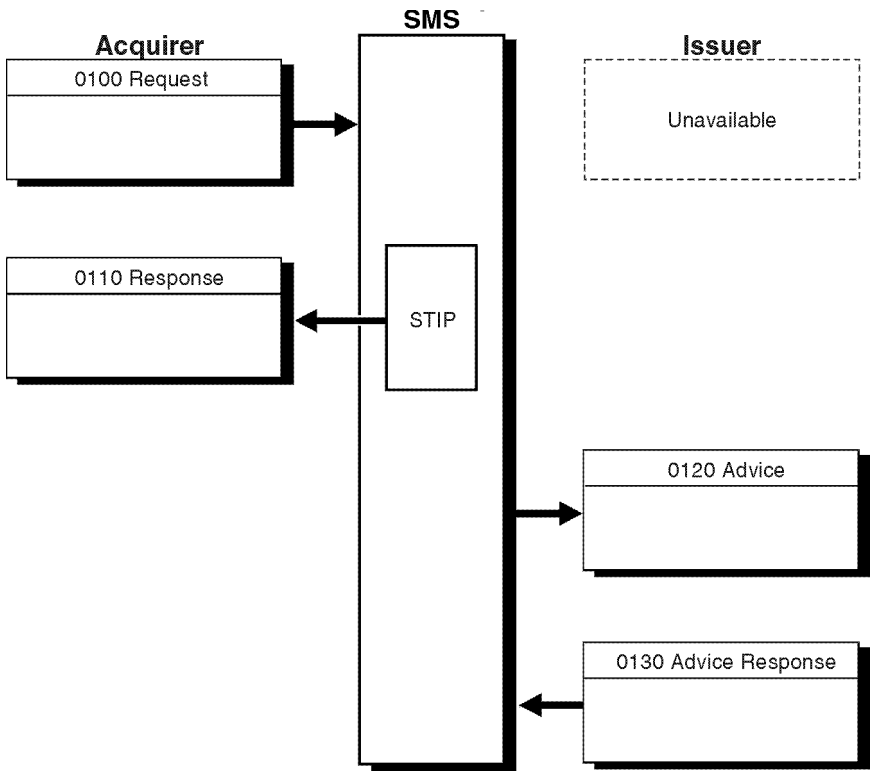
Exception condition processing for authorizations applies to Visa and Visa Electron only.

Authorization—Issuer Unavailable

Figure 4–26 illustrates an authorization in which the issuer is not available, and STIP responds on behalf of the issuer.

Visa	✔
Visa Electron	✔

Figure 4–26: Authorization—Issuer Unavailable 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

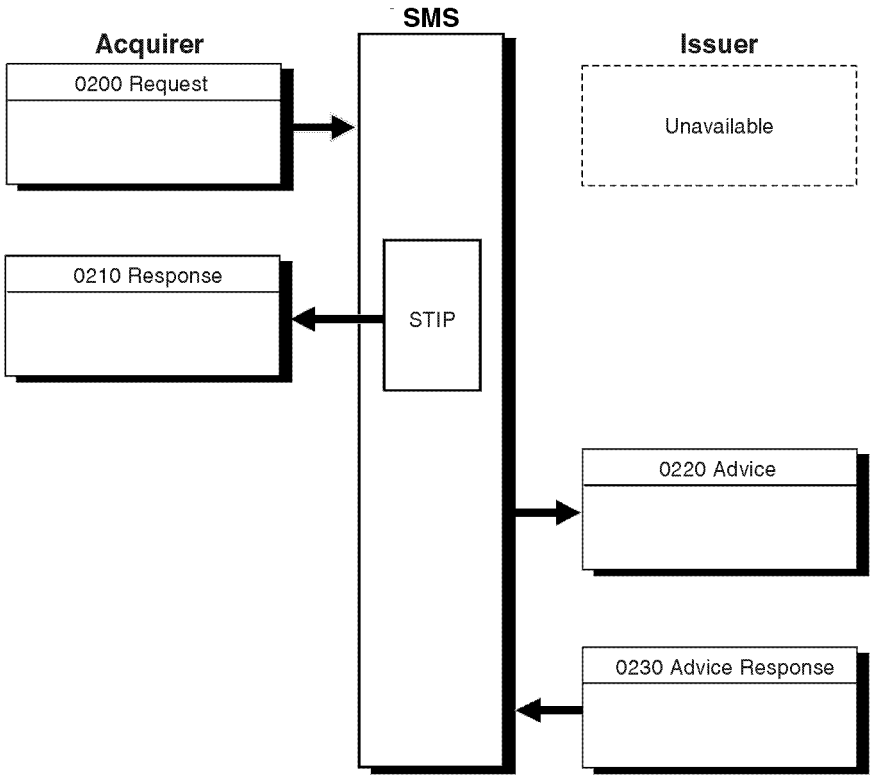
If the issuer is unavailable, STIP responds to the 0200 request and creates an 0220 advice for the issuer to recover. This advice reflects both the request and the STIP reply. When the issuer recovers the 0220 advice, it acknowledges with an 0230 advice response.

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

Figure 4–27 illustrates stand-in processing for an issuer that is unavailable to send a response to an acquirer's authorization request.

Visa	✔
Visa Electron	✔

Figure 4–27: Issuer Unavailable Transaction Flow



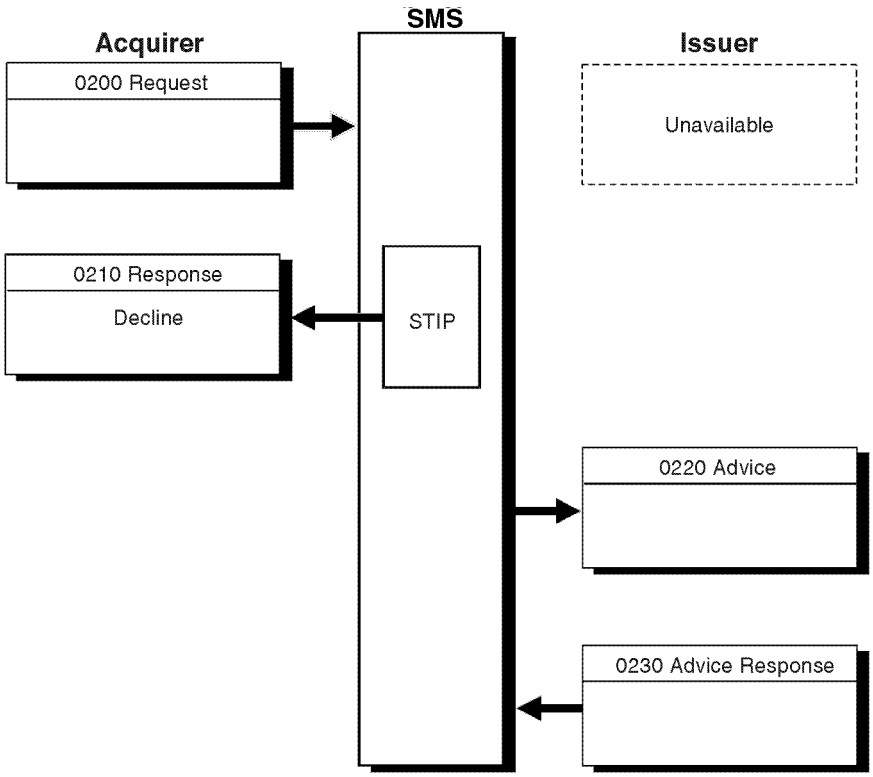
Issuer Unavailable—Account Listed on Exception File

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.

Figure 4–28 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.

Visa	✔
Visa Electron	✔

Figure 4–28: 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 (Auto-CDB) Update service, 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.

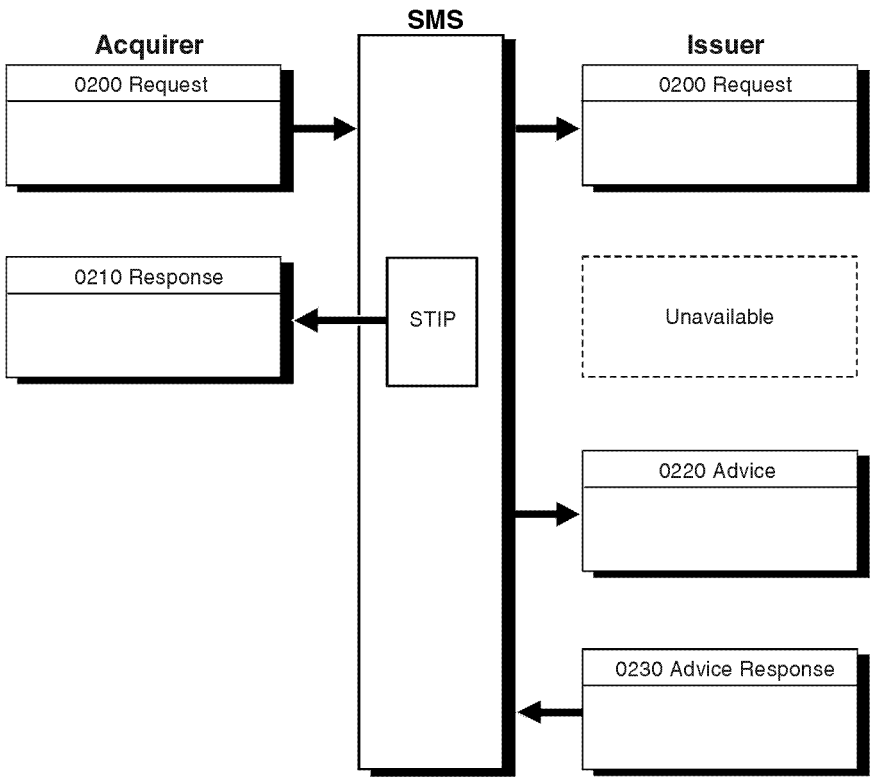
Issuer Fails to Respond

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 4–29 illustrates STIP standing in when the issuer has received the request but is unable to respond before a timeout has occurred.

Visa	✔
Visa Electron	✔

Figure 4–29: 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:

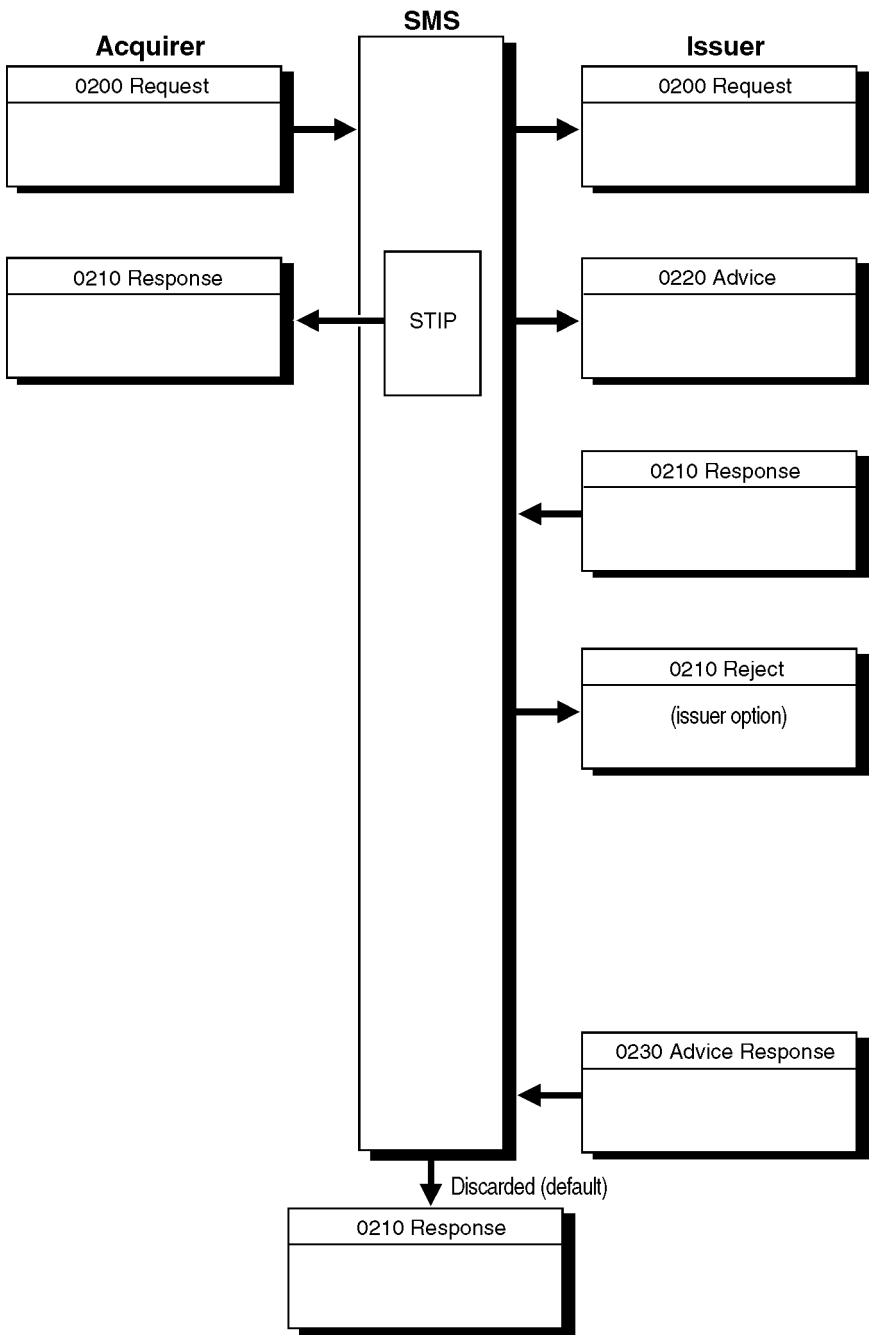
- Reject the 0210 response with a reject code of 515 (late response) in the reject header. This is an issuer-selected option.
- Discard the 0210 response. This is the default option.

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 4–30 illustrates STIP standing in when the issuer has received the request but responds late.

Visa	✔
Visa Electron	✔

Figure 4–30: 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.

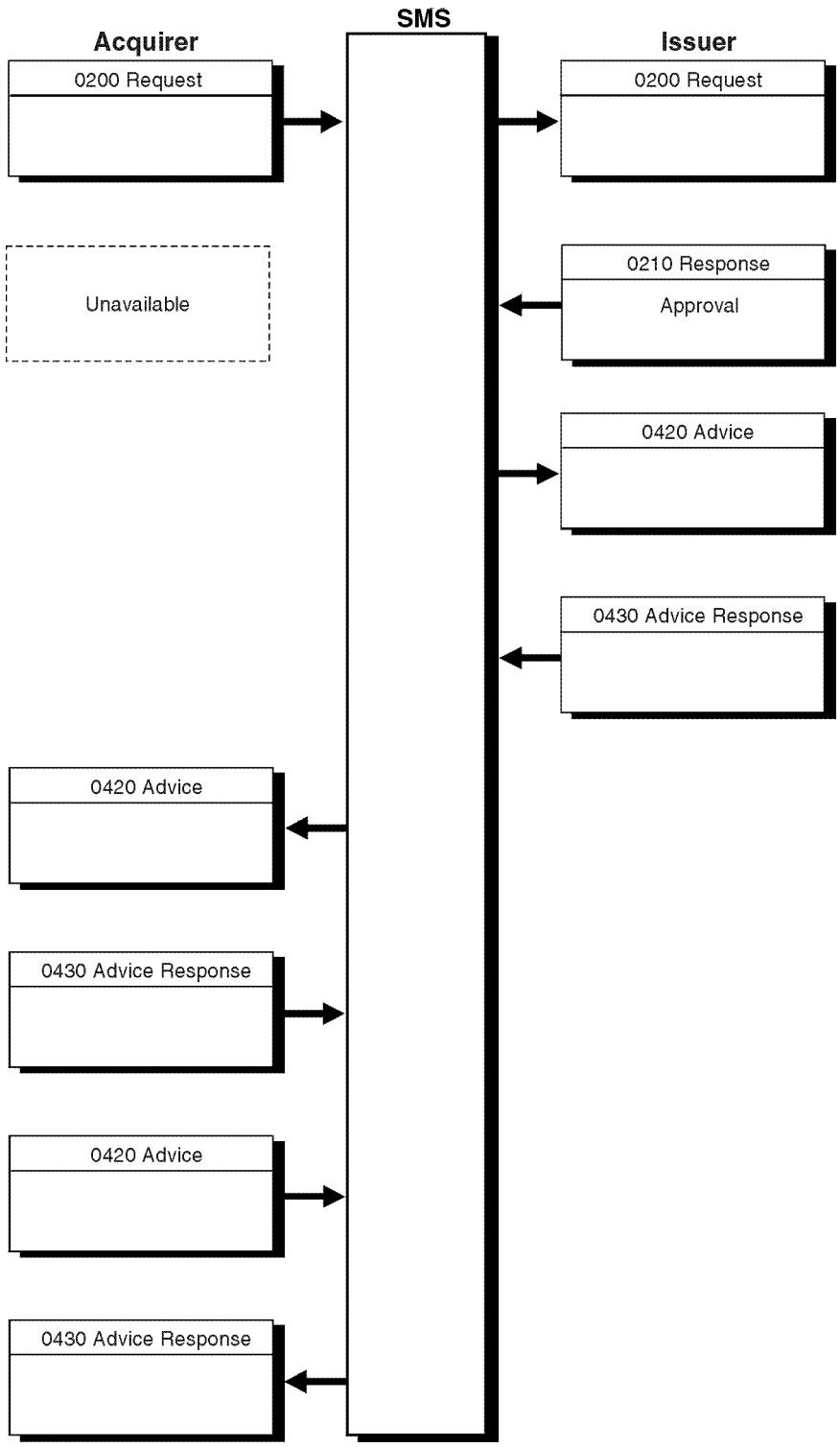
If SMS has not reversed the 0200 already, then the acquirer's 0420 will be treated like a normal reversal and will go through to the issuer.

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

Figure 4–31 illustrates the transaction flow of an approval that cannot be delivered to the acquirer.

Visa	✔
Visa Electron	✔

Figure 4–31: 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.

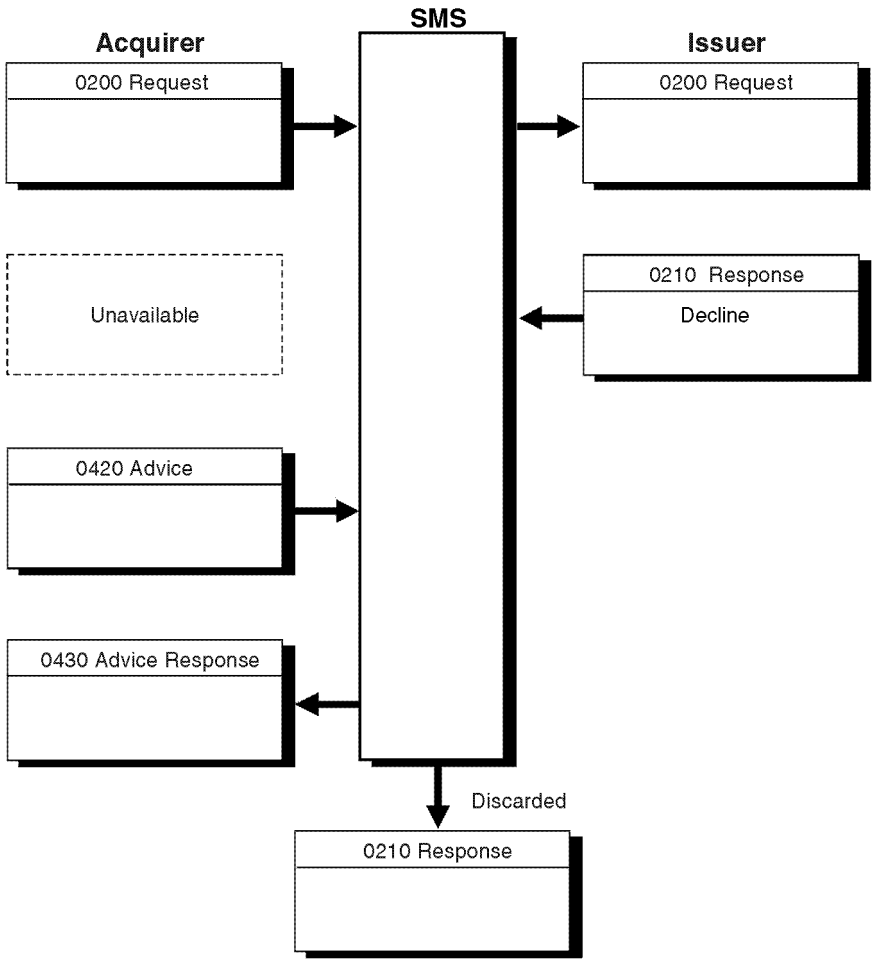
The acquirer must send an 0420 reversal advice to SMS after determining that an 0210 response has not been received. SMS acknowledges with an 0430 advice response that contains an approval response code. SMS also sets Gross Interchange Value Update Flag to zero, indicating that the reversal has no financial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

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

Figure 4–32 illustrates the transaction flow of a decline response that cannot be delivered to the acquirer.

Visa	✔
Visa Electron	✔

Figure 4–32: 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

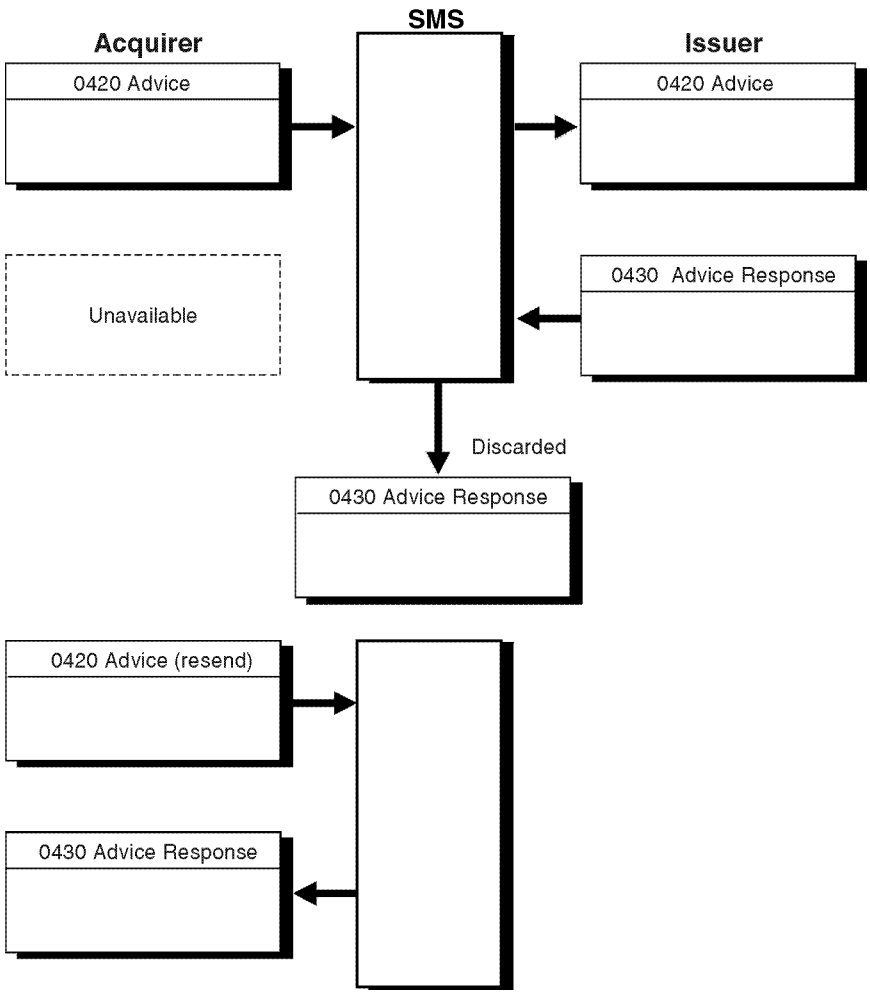
Reversal—Advice Response Cannot Be Delivered to the Acquirer

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 4–33 illustrates the transaction flow of an advice that cannot be delivered to the acquirer.

Visa	✔
Visa Electron	✔

Figure 4–33: Reversal—Advice Response Cannot Be Delivered to the Acquirer Transaction Flow



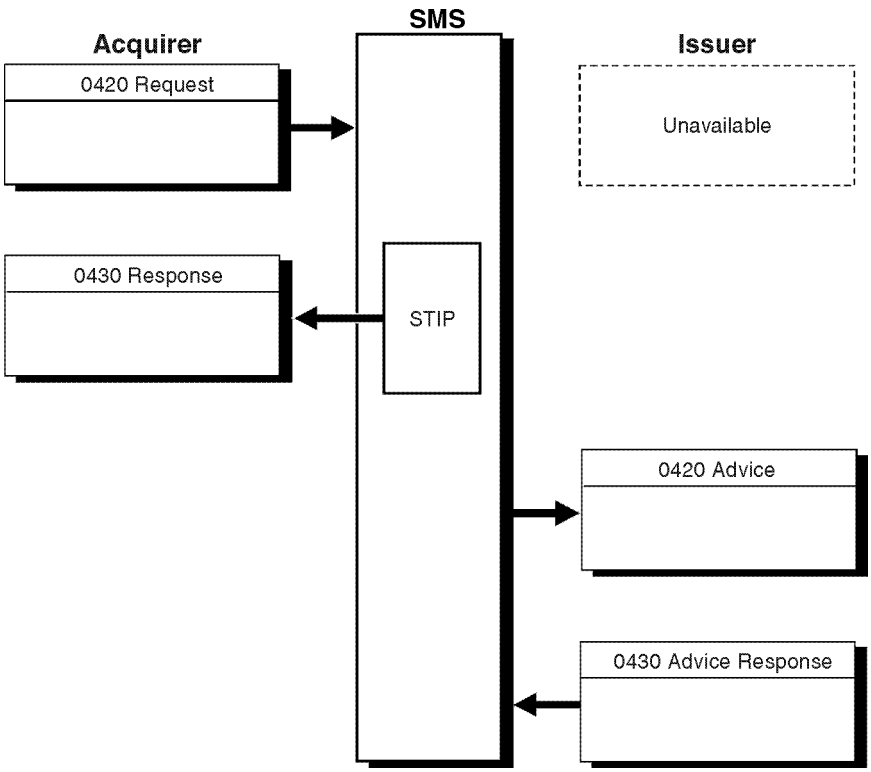
Reversal—Issuer Unavailable

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 4–34 illustrates the transaction flow of a reversal when the issuer is not available.

Visa	✔
Visa Electron	✔

Figure 4–34: Reversal—Issuer Unavailable Transaction Flow



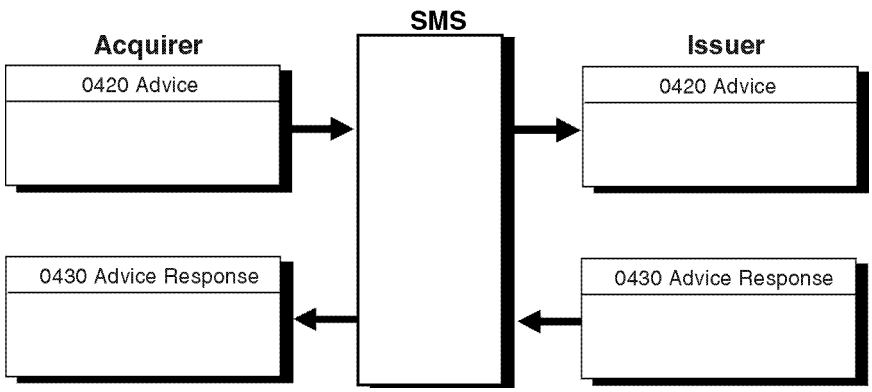
Reversal—Unsolicited

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 4–35 illustrates the transaction flow for an unsolicited reversal.

Visa	✔
Visa Electron	✔

Figure 4–35: 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.

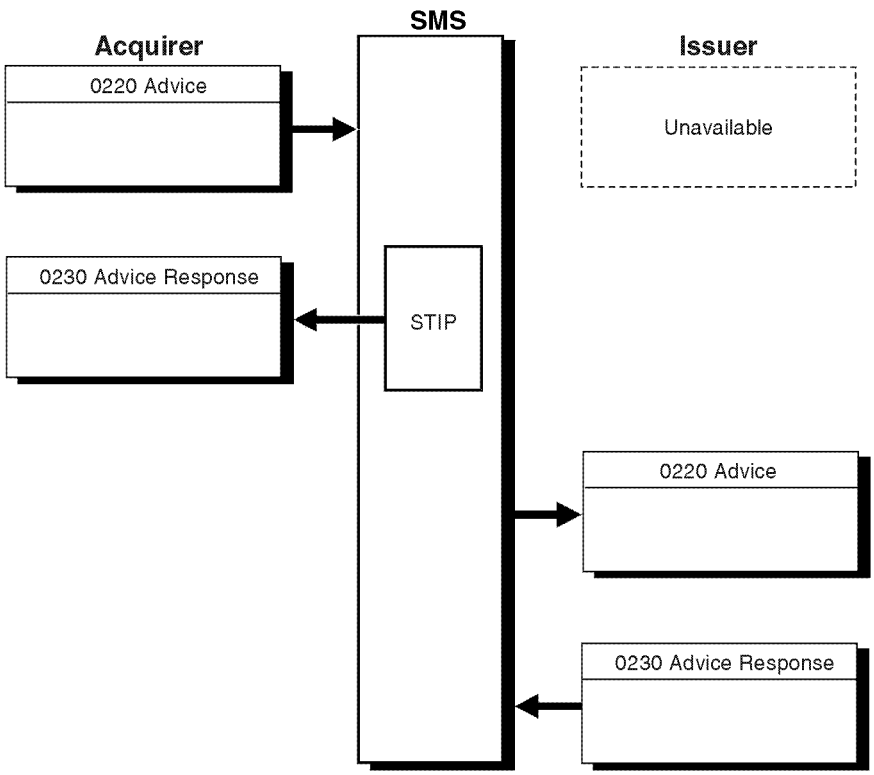
Adjustment or Representment—Issuer Unavailable

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.

Figure 4–36 illustrates an adjustment or representment transaction flow when the issuer is unavailable.

Visa	✔
Visa Electron	✔

Figure 4–36: Adjustment or Representment—Issuer Unavailable Transaction Flow



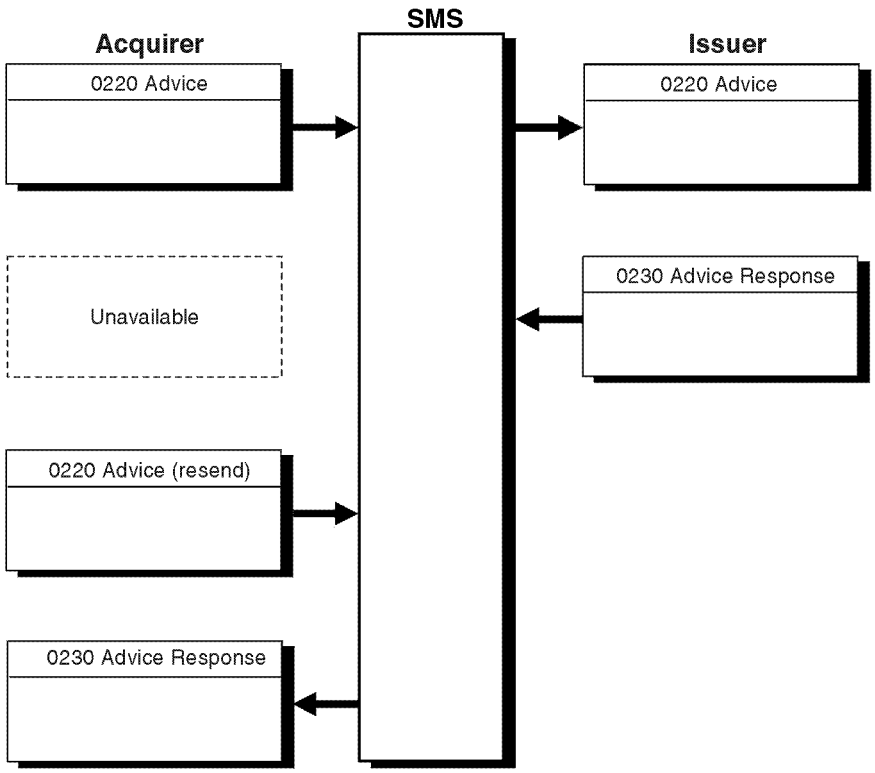
Adjustment or Representment—Acquirer Unavailable After Advice

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 builds a response to the acquirer as though the duplicate advice were the original transaction.

Figure 4–37 illustrates an adjustment/representment transaction flow when the acquirer is unavailable.

Visa	✔
Visa Electron	✔

Figure 4–37: Adjustment or Representment—Acquirer Unavailable Transaction Flow



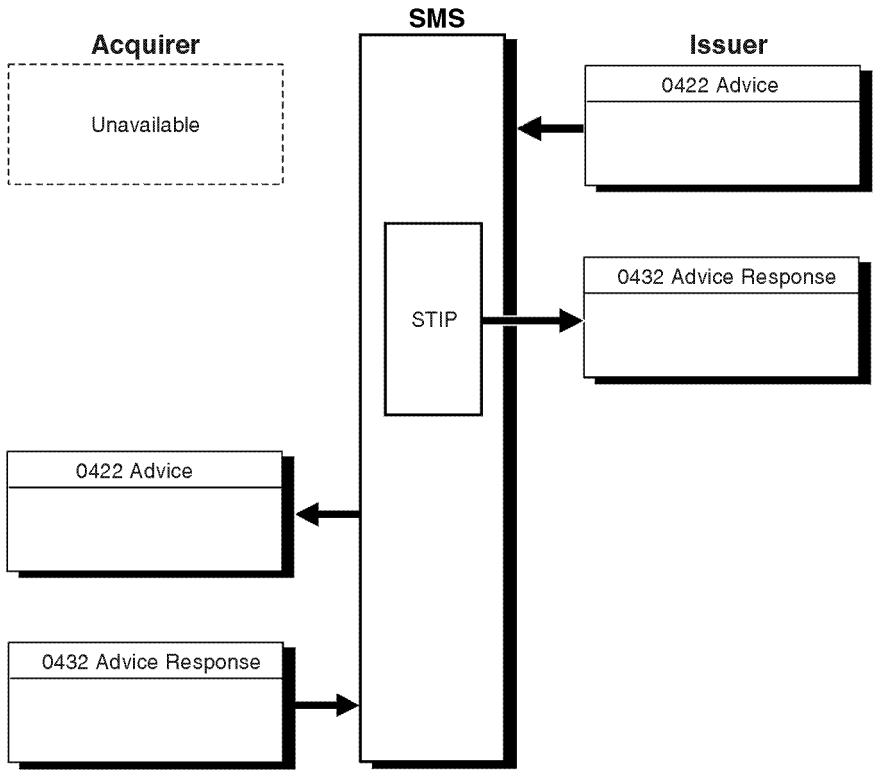
Chargeback—Acquirer Unavailable

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 4–38 illustrates STIP authorizing a chargeback.

Visa	✔
Visa Electron	✔

Figure 4–38: Chargeback—Acquirer Unavailable



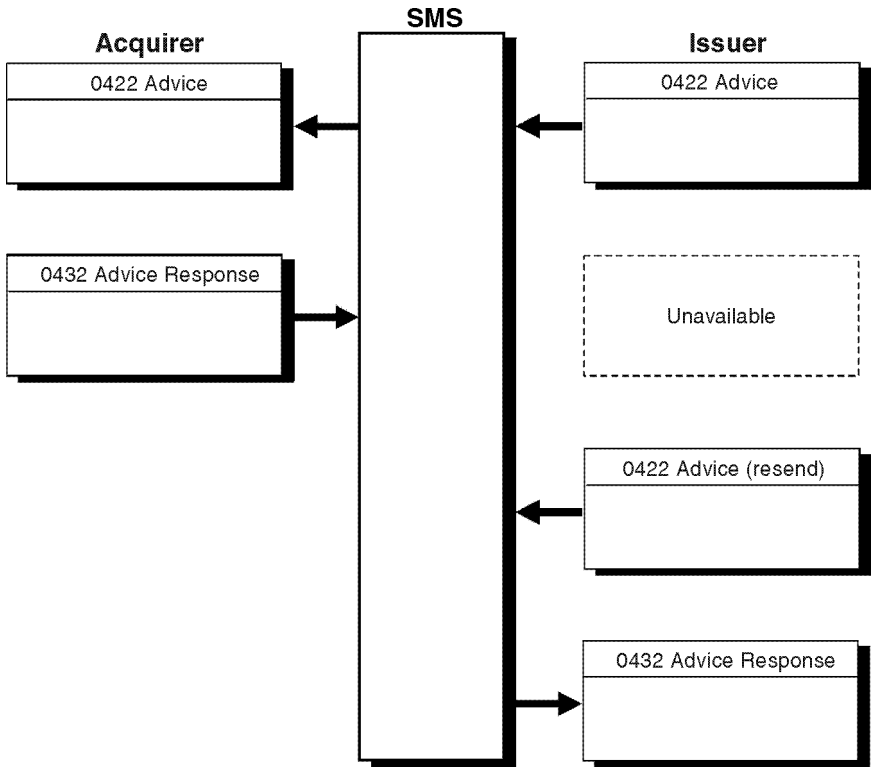
Chargeback—Issuer Unavailable After Chargeback

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 4–39 illustrates the transaction flow of an issuer unavailable after a chargeback.

Visa	✔
Visa Electron	✔

Figure 4–39: Chargeback—Issuer Unavailable After Chargeback Transaction Flow



Multicurrency Support 5

Participation in the Multicurrency Service is a requirement for Visa POS and global Electron members outside of the United States (U.S.) region.

The V.I.P. SingleConnect POS Service features full *multicurrency support* for international VISA POS and Electron transactions. 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 online 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.
- 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 POS (Visa & Visa Electron) 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 on a given day, the components might be as follows:

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.*

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.

Variations

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

- For the following transactions, SMS uses the currency conversion procedure described in the "How Currency Conversion Works" section of this chapter with the current day's base rate plus the Visa currency conversion fee and the optional issuer fee:
  - Manual cash disbursement
  - Authorization
  - Purchase
  - Adjustment
  - Representment

  Note that "current day's base rate" means the rate in effect on the day SMS receives the transaction.

- For *reversals*, 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.
- 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 *chargeback reversals*, SMS uses the base rate that was in effect at the time of the chargeback, without calculating the currency conversion fees and optional issuer fees.
- For *merchandise returns*, SMS calculates the currency conversion fees and subtracts the fees from the cardholder billing amount.

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, one, 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 POS (Visa & Visa Electron) 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

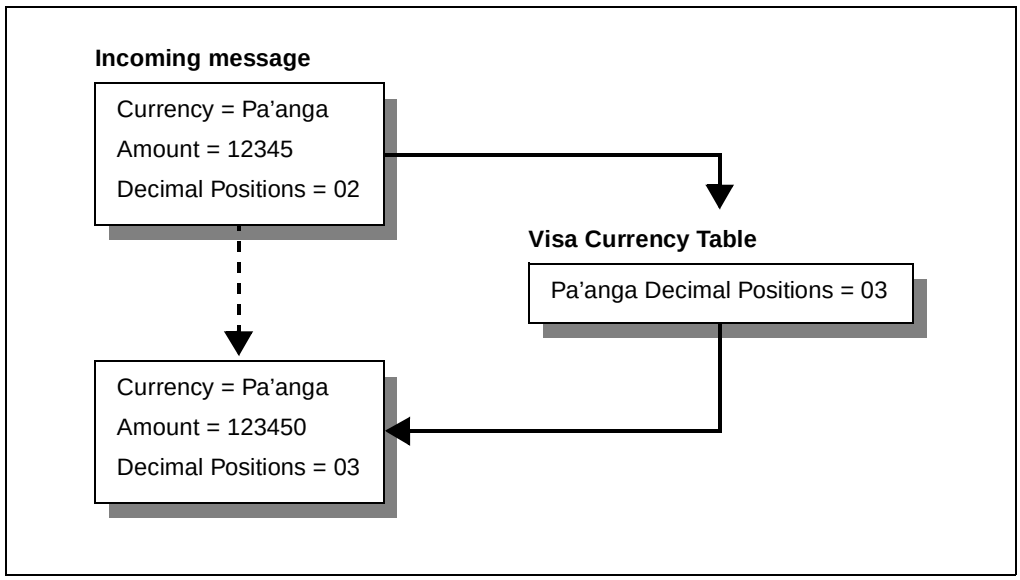
An acquirer sends a transaction amount of 12345 and places 02 in positions 1 and 2 of the Decimal Positions Indicator field. However, the Currency Table indicates that the currency has three decimal positions. Visa reports the amount as 123450 and sends the issuer a transaction amount of 123450.

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

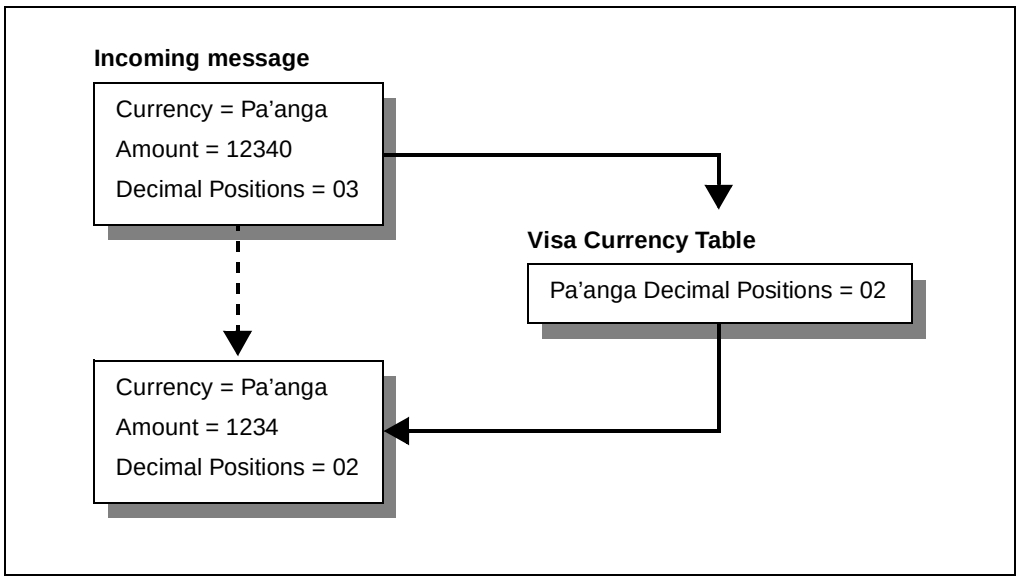
If the number of decimal positions specified in field 63.13 is greater than that in the table, the last digit (which must be zero) is removed.

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 nonparticipating member is not receiving the enhanced data fields.
- The U.S. acquirer that does not participate in the Multicurrency Service can 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 the 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:

- Authorization Transaction (Figure 5–3)
- Purchase Transaction (Figure 5–4)
- Adjustment Transaction (Figure 5–5)
- Representment Transaction (Figure 5–6)
- Reversal Transaction (Figure 5–7)
- Chargeback and Chargeback Reversal Transaction (Figure 5–8)
- Merchandise Return Transaction (Figure 5–9)

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 point of sale has a local currency of Japanese yen, the cardholder is billed in Australian dollars, the acquirer receives the settled amount in U.S. dollars, and the issuer settles 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 3—Processing Code

Field 4—Amount, Transaction

Field 5—Amount, Settlement

Field 6—Amount, Cardholder Billing

Field 9—Conversion Rate, Settlement

Field 10—Conversion Rate, Cardholder Billing

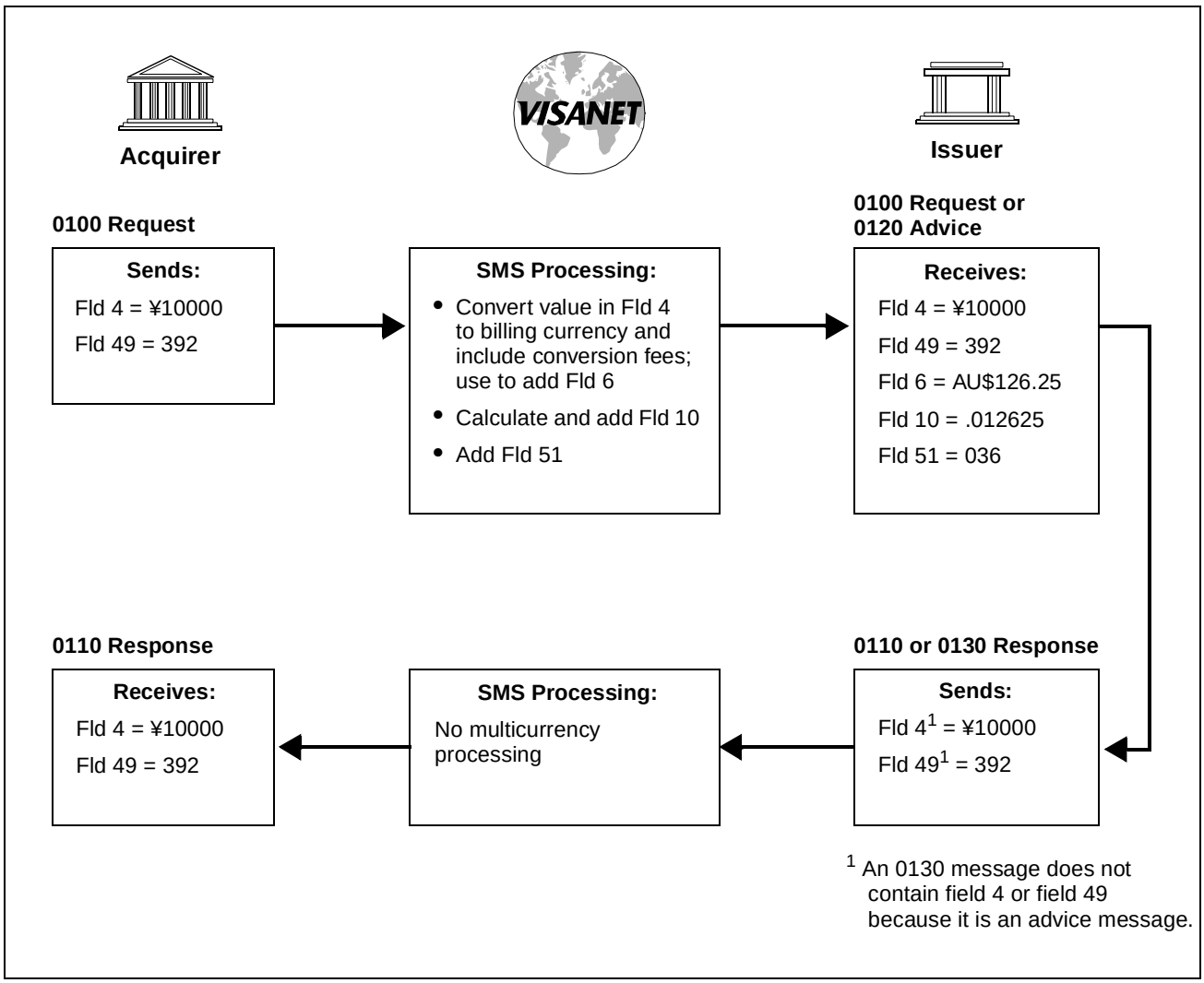
Field 16—Date, Conversion

Field 49—Currency Code, Transaction

Field 50—Currency Code, Settlement

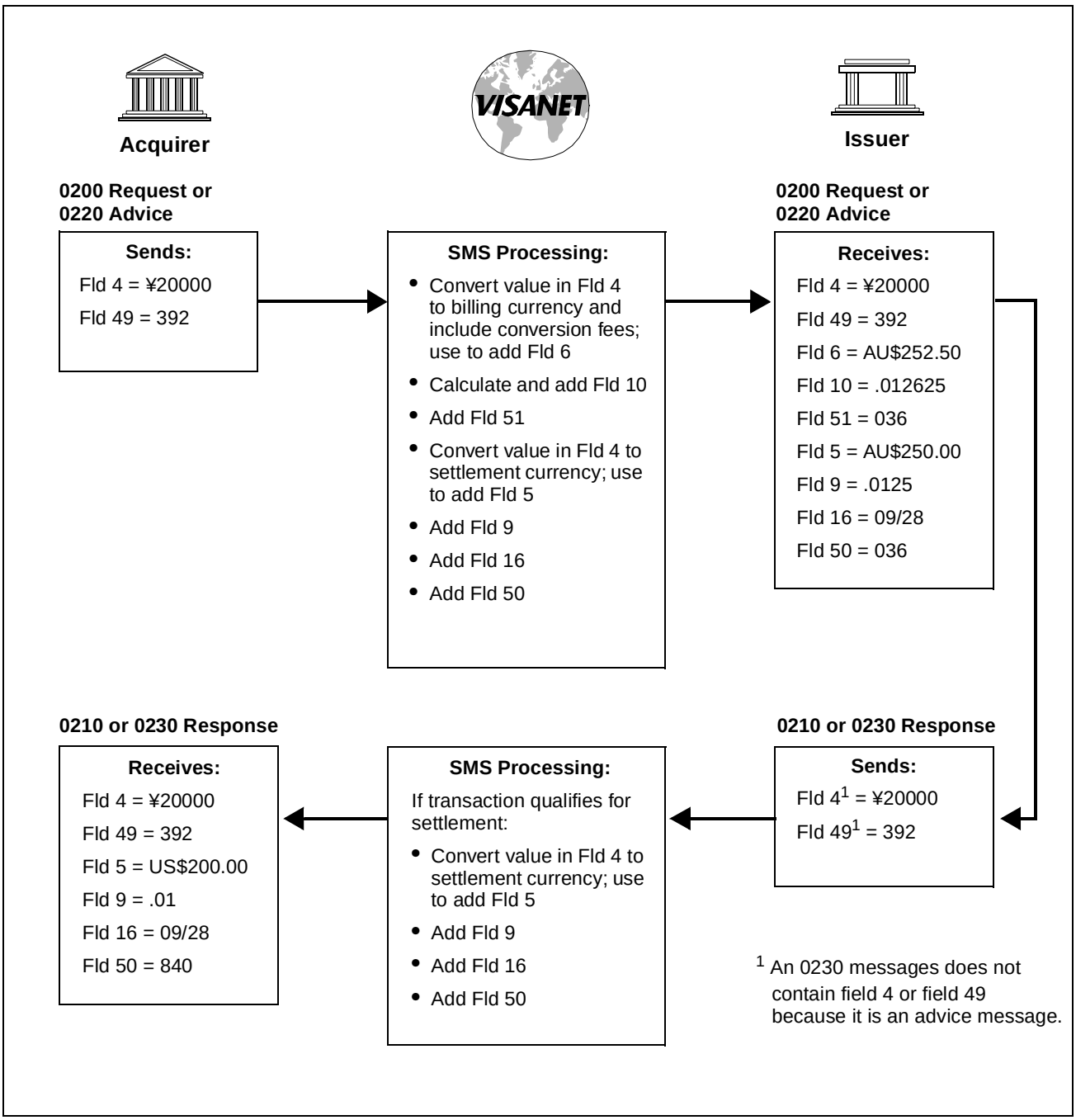
Field 51—Currency Code, Cardholder Billing

Figure 5–3: Authorization Transaction



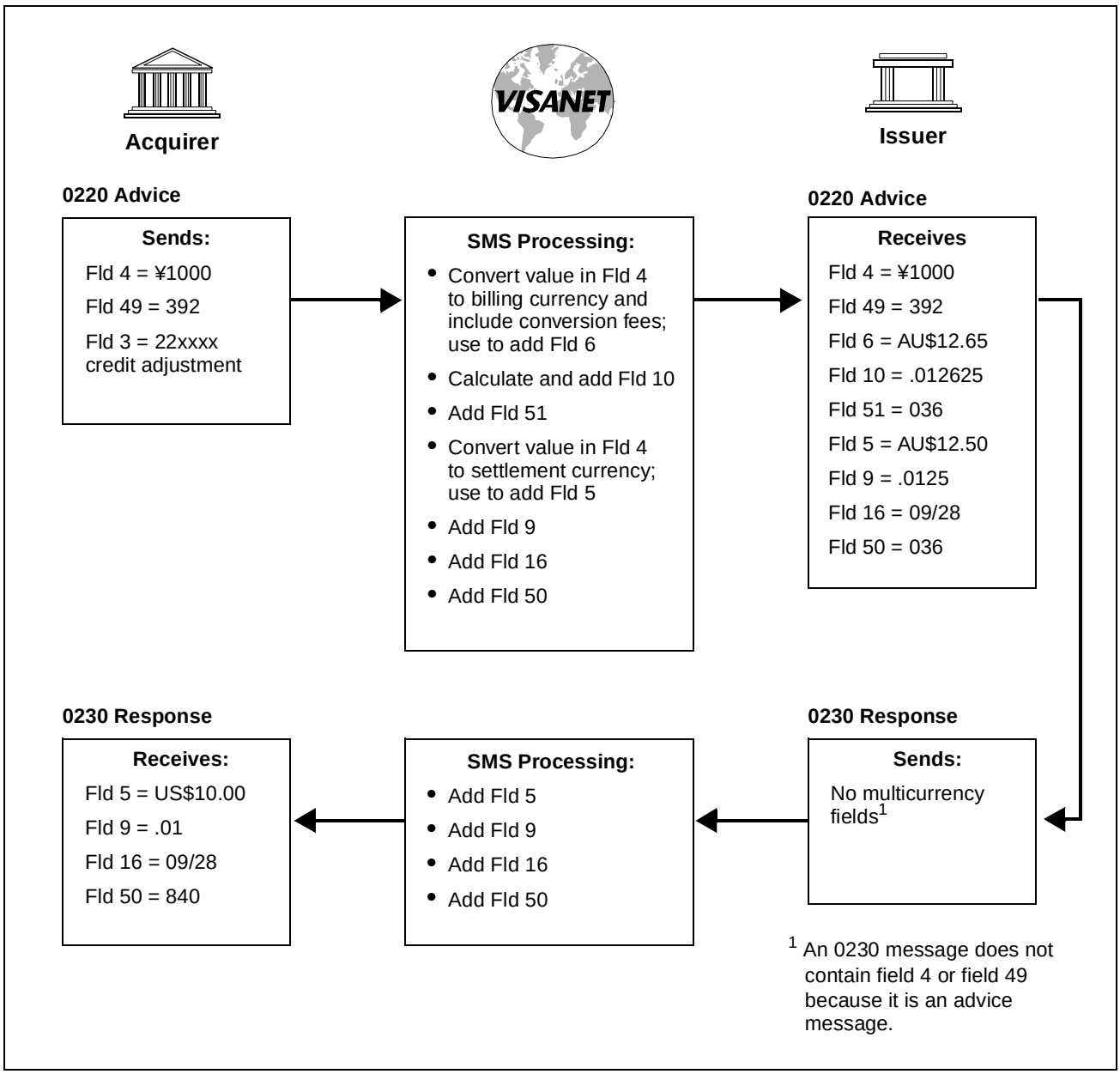
For this example, ¥100 = US$1.00 and AU$1.25 = US$1.00.

Figure 5–4: Purchase Transaction



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

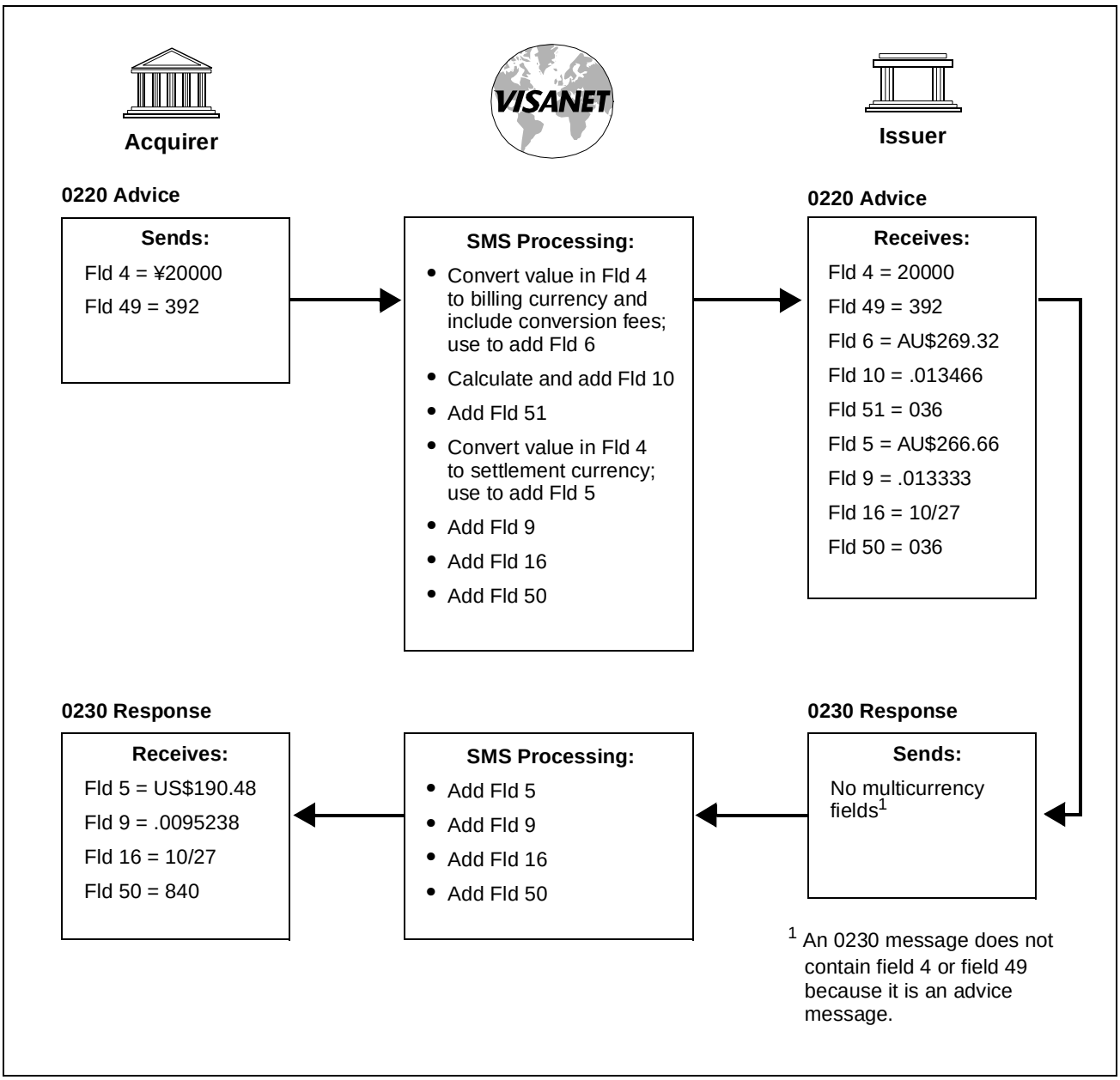
Figure 5–5: Adjustment Transaction



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

Currency conversion rates used for a back office adjustment can differ from the rates used for the original transaction.

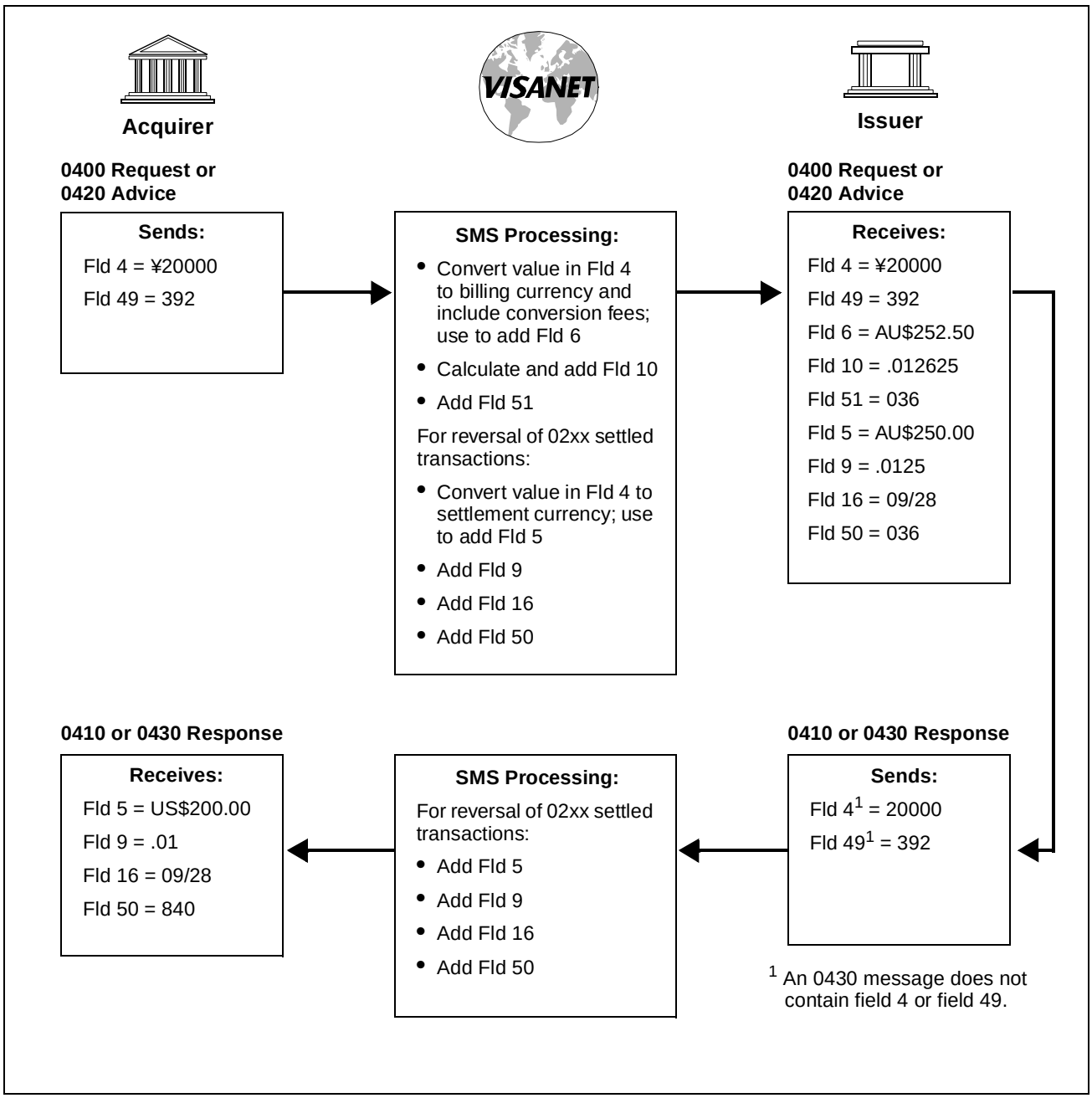
Figure 5–6: Representment Transaction



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

This example illustrates that the currency conversion rates used for a representment can differ from the rates used for the corresponding chargeback. (See the rates used in the chargeback example in Figure 5–8.)

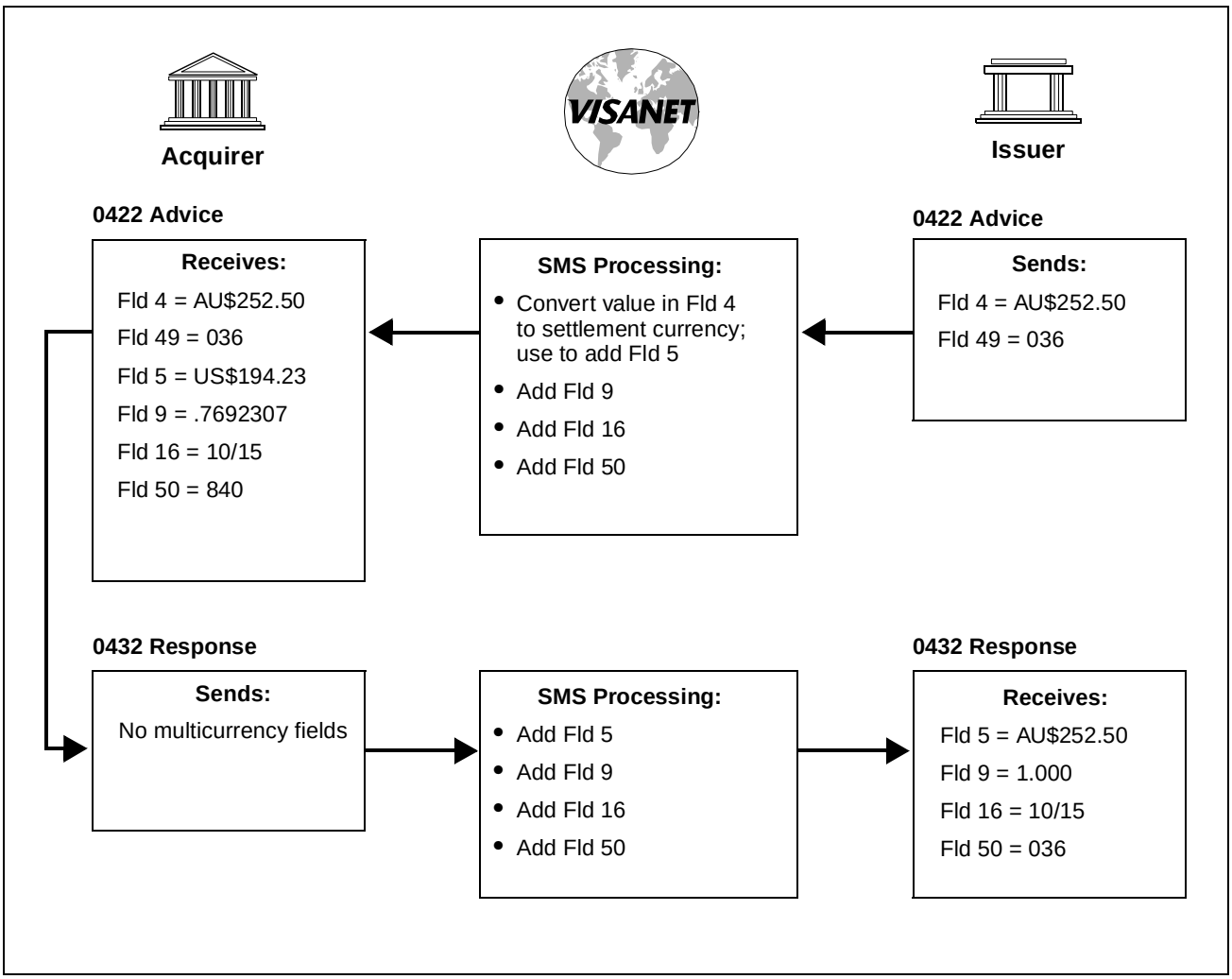
Figure 5–7: Reversal Transaction



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

Under normal circumstances, the acquirer sends an 0420 request to the issuer. Because pre-existing acquirers can also generate 0400 request messages, issuers respond with 0410 messages that include field 4 and field 49.

Figure 5–8: Chargeback and Chargeback Reversal Transaction

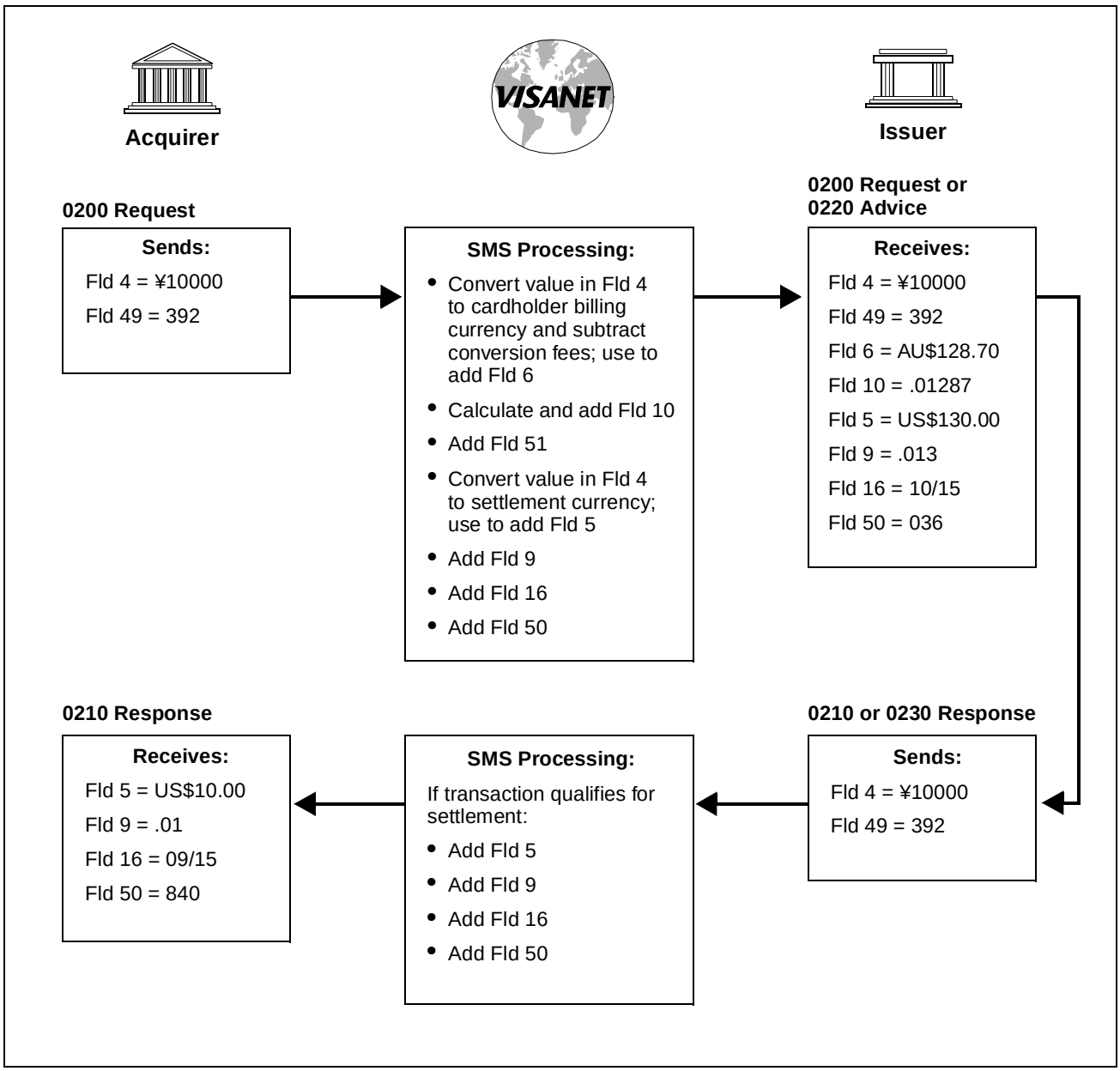


For this example, AU$1.30 = US$1.00.

The issuer provides the chargeback amount in the cardholder billing currency as it was received in field 6 of the original request or advice.

This example illustrates that the currency conversion rates for a chargeback can differ from the rates used for the original financial transaction.

Figure 5–9: Merchandise Return Transaction



For this example, ¥100 = 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.
- Other risk 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.
- 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 issuer responds with Response Code 91—Destination Unavailable (an issuer option).

Issuer STIP Options

The options that issuers can specify for STIP are the following:

- 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 pick-ups or 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 and CVV2) services
- Having STIP decline all transactions when the issuer is not available

STIP Authorization Processing

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

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

- Edit check

- Exception File check
- PIN verification
- Activity check

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.

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.

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. Issuers must use a value not greater than 20 years from the issue date.

Visa cards must contain standard data in track 1 and track 2. Card expiration dates in requests 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.

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 POS (Visa & Visa Electron) 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 and Manual Cash Disbursements

STIP checks purchases and manual cash disbursements 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:

04 = Pick up (nonfraud); does not apply to Interlink.

05 = Do not honor.

07 = Pick up, special condition (fraud); does not apply to Interlink.

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.

41 = Lost card; pick up (fraud).

43 = Stolen card; pick up (fraud).

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.

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 and the PIN Verification Service, refer to Chapter 7, Security.

Activity Check

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

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—Approved 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 POS (Visa & Visa Electron) Technical Specifications.*

Updating the Activity File

When STIP approves a financial transaction, STIP updates the transaction totals in the cardholder's activity record. For financial requests and reversals, STIP updates:

- The count and amount totals for the approved request.
- The cardholder's grand 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 POS (Visa & Visa Electron) 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 an authorization 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 POS (Visa & Visa Electron) 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 also are 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 the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron) Technical Specifications*.

Positive Authorization Capacity Management (PACM) Service

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.

Participation in PACM is optional for issuers. PACM is available for Visa and Visa Electron transactions, including Visa Secure Electronic Commerce (VSEC) transactions.

For a comprehensive description of this service, 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: Acquirer Advices

Issuer-Generated Request	STIP Advice to Acquirer
Chargeback (0422)	Chargeback (0422)
Chargeback Reversal (0422)	Chargeback Reversal (0422)
Copy Request (0600)	Copy Request Advice (0620)
Text Message (0600)	Text Message Advice (0620)
Fee Collection or Funds Disbursement (0422)	Fee Collection or Funds Disbursement (0422)

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 the acknowledgment of advices or sign-on messages.
- 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, as 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
- BASE II transaction advices
- CRIS alerts (if member participates)

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.

➤ 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 then 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:

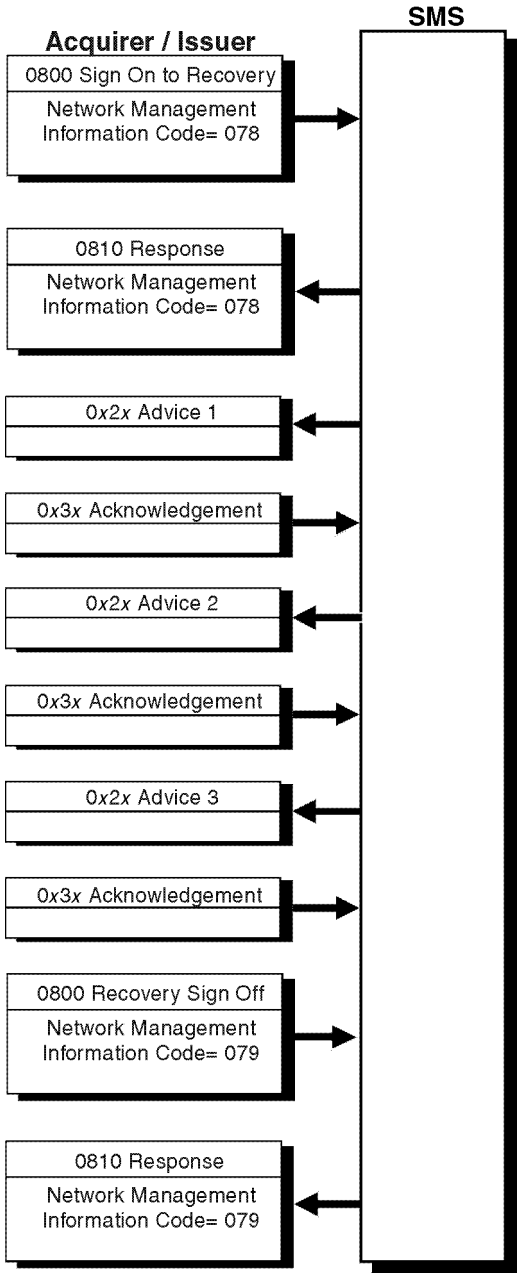
1. The issuer sends an 0800 message containing the applicable Network Management Information Code 079.
2. SMS replies with an 0810 response.

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

IMPORTANT

The member should remain signed on during this process.

Figure 6–1: Advice Recovery Flow



Advice Flags in the Message Header

To provide additional information, Header Field 9—Message Status Flags 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 POS (Visa & Visa Electron) Technical Specifications.*

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 issuers of Visa card products. All Visa card products (Visa Classic, Visa Gold, Visa Business, Visa Corporate, Visa Purchasing, and Visa Electron) must be encoded with CVVs.

NOTE: *The CVV Service provides no support for POS transactions using proprietary cards.*

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 1 and track 2.

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

A transaction is eligible for CVV checking when:

- Both the acquirer and the issuer are CVV participants
- The transaction contains a value of “90” 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 VisaNet 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 1 and track 2 data
- Incorrect encoding of CVV, such as an incorrect position or wrong key

Issuers who do not participate in the CVV Service may *not* exercise the magnetic stripe counterfeit transaction chargeback (chargeback reason code 62).

Acquirers are subject to magnetic-stripe counterfeit transaction chargebacks if any of the following conditions are true:

- Acquirer is not participating
- Acquirer is participating but the transaction did not carry full, unaltered magnetic stripe data
- Acquirer is participating but transaction did not indicate the magnetic stripe data was full and unaltered

Issuer Processing Options

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

- VisaNet CVV validation
- Receiving CVV results
- CVV default response codes

VisaNet CVV Validation

Three VisaNet 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 eligible 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, VisaNet responds to the acquirer using the issuers'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 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 "82" (CVV Validation Failure) 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.

The issuer can also optionally send the CVV results of tests conducted by VisaNet or the issuer 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 who 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 VisaNet 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)

01 = refer to issuer

04 = pick up

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.*

CVV Transaction Processing

Table 6–3 summarizes the processing that occurs for each transaction type for issuers participating in the CVV Service.

Table 6–3: CVV Transaction Processing Summary (1 of 2)

Transaction Type	For Participating Issuers		
	VisaNet Processing—Issuer Unavailable	**VisaNet Processing—Issuer Available**	**Issuer Processing**
Purchases (0200); Purchases with cashback (0200); Merchandise Return (0200); Manual Cash Disbursement (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 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, 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 Issuers perform standard authorization processing, taking into consideration the CVV results. At the issuer's option, the issuer provides CVV results in field 44.5.

Table 6–3: CVV Transaction Processing Summary (2 of 2)

Transaction Type	For Participating Issuers		
	VisaNet Processing—Issuer Unavailable	**VisaNet Processing—Issuer Available**	**Issuer Processing**
Reversals (0400, 0420)	VisaNet does not perform CVV validation. The does not contain CVV validation information.	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.

Issuer Requirements

The issuer who participates in the CVV Service is responsible for calculating the CVV on track 2 of the magnetic stripe and for providing Visa with the keys used for calculating the CVV.

Calculating and Encoding the CVV

Participating issuers must encode the CVV on the magnetic stripes 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 interfaces to 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.

The issuer must encode the CVV on both track 1 and track 2 of the magnetic stripe, and the value must be the same on both tracks. For more information on calculating and encoding the CVV, see the *Card Technology Standards Manual*.

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. 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 verification 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 be able to 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 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 (such as credit-worthiness or funds on account).

- ¤ Field 44.5—CVV Results Code should contain the value “2” (transaction passed CVV validation).

– If the CVV is invalid:

- ¤ A Referral (01), Pick Up Card (04), or Decline (05) response code should be generated.
- ¤ Field 44.5—CVV Results Code should contain the value “1” (transaction was checked for CVV and failed verification).

- If field 22 contains a value of “02” (magnetic stripe read), the issuer should not perform CVV validation.

Acquirer Processing Options

To manage possible terminal or line problems, acquirers have the option to receive Field 44.5—CVV Results Data in authorization and financial message responses. If the issuer does not provide the results in field 44.5, the results are not be available to the acquirer. Results are provided to the participating acquirer when transactions have been processed in stand-in.

When requesting CVV results, the acquirer receives a value 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.

It is Visa’s policy that CVV results are not returned to the point of sale.

Acquirer Requirements

Acquirers participating in the CVV Service must be able to transmit the entire contents of the magnetic stripe from their merchants’ terminals and must do so without alteration or truncation of the data.

Acquirers indicate that the complete unaltered magnetic stripe is included in the authorization request by:

- Placing a value of "90" (magnetic stripe read and the entire contents transmitted) in the first two positions of Field 22—Point of Service Entry Mode Code.
- Including either Field 35—Track 2 Data or Field 45—Track 1 Data in the request when the POS Entry Mode Code field indicates that the data is obtained from reading the magnetic stripe.

Acquirers without the capability to read and transmit the entire contents of the magnetic stripe should send the value "02" (magnetic stripe read) in field 22.

NOTE: *If the acquirer converts track 1 data to track 2 data, the acquirer must use "02" in field 22, as the contents of the magnetic stripe have been altered.*

CVV Certification

Both acquirers and issuers must be certified to participate in the CVV Service.

Acquirers must certify online for the POS Entry Mode Code 90 and the transmission of the entire unaltered contents of the magnetic stripe (including track 1 and track 2 data).

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 or acquirer 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 acquirer or 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

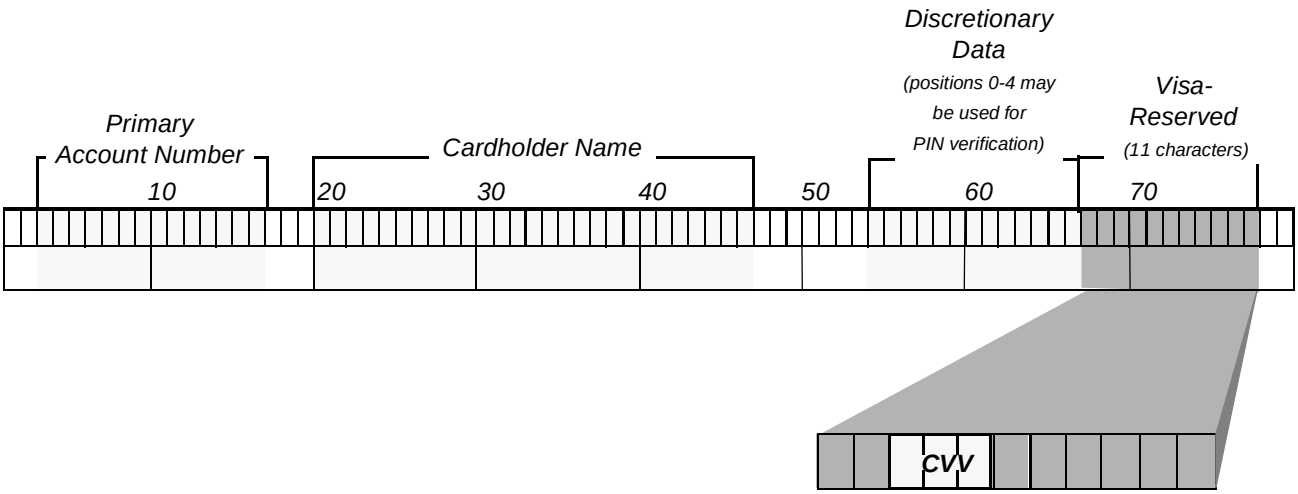
The CVV must be encoded on track 1 and track 2 of the magnetic stripe, and the value must be the same on both tracks. The placement on each track is as follows.

Placement on Track 1

The three-character CVV for track 1 is placed in the Visa-Reserved field of the stripe. This field is eleven characters long, and the CVV must be placed in positions 3, 4 and 5, as shown in Figure 6–2. With the exception of position 8, the remainder of this field should be zero-filled (position 8 may contain the Authorization Control Indicator (ACI); otherwise it should also be zero-filled). Refer to the *Card Technology Standards Manual* for specific format information of track 1. Issuers may also encode the CVV anywhere else in the track 1 Discretionary Data field for internal use.

Figure 6–2 illustrates a track 1 with a 16-digit primary account number and a 26-position cardholder name.

Figure 6–2: Placement of CVV on Track 1



Placement on Track 2

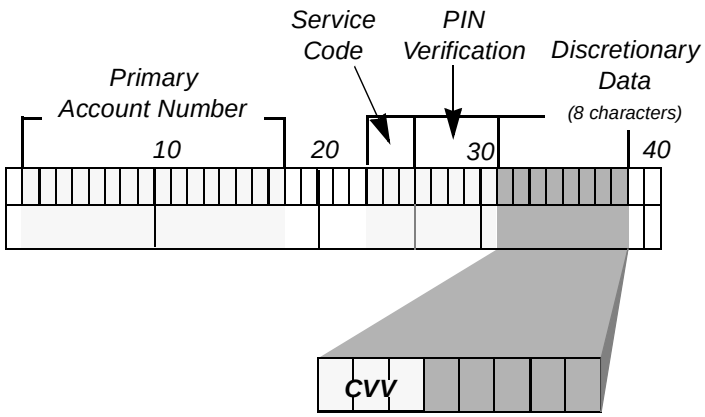
The CVV can be placed anywhere in the Discretionary Data field of track 2. The issuer must inform Visa of the CVV location by indicating the number of positions it is displaced from the end of the Service Code field (the first position of the displacement 0).

Note the following differences when using 13- and 16-digit account numbers:

- For 13-digit account numbers, the CVV for PIN Verification Service (PVS) users who encode their cards with the PVV may begin anywhere between positions 5 to 13. Non-PVS users may begin the CVV anywhere from positions 0 to 13.
- For 16-digit account numbers, the CVV for PIN Verification Service (PVS) users who encode their cards with the PVV may begin anywhere between positions 5 to 10. Non-PVS users may begin the CVV anywhere from positions 0 to 10.

In Figure 6–3, the displacement is 5 because the PIN Verification field is present. If the PIN Verification field was not present, the displacement would be 0 (zero). The Discretionary Data field may be eight digits (if the PIN Verification field is present), as in Figure 6–3, or thirteen digits (if the PIN Verification field is not present). Refer to the *Card Technology Standards Manual* for specific format information for track 2.

Figure 6–3: Placement of CVV on Track 2



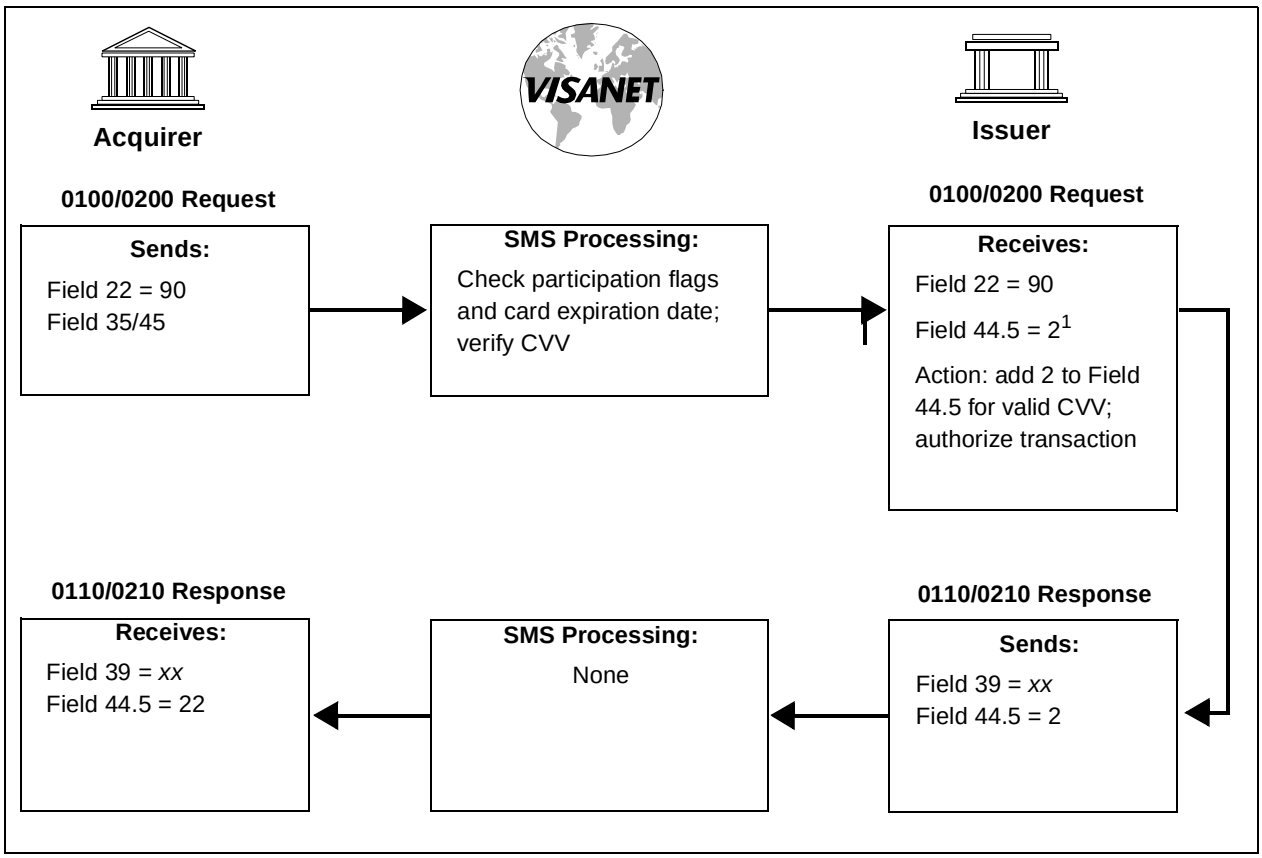
CVV Flow

The flow shown in Figure 6–4 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 6–4: CVV Flow Example



[1] Only if the issuer has opted to receive the CVV Results Code 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 CVV2 Service is a card verification tool designed to reduce fraud losses on transactions when the card is not present. The CVV2 service is available for all SingleConnect issuers and acquirers.

Issuers indent-print a Card Verification Value 2 (CVV2) on the back of a Visa card using a reverse italic font. All Visa cards (including emergency replacement cards) must carry the CVV2 security number. Issuers generate the CVV2 values using Data Encryption Standard (DES) keys and an algorithm.

To verify the CVV2, V.I.P. uses the DES key and other CVV2 parameters provided by participating issuers to calculate the CVV2 value and compare it with the card's printed CVV2. If V.I.P. or the issuer generates a CVV2 "no match" result, V.I.P. assigns CVV2 Result Code "N"—No Match to the transaction. V.I.P. forwards the result to the issuer. The issuer optionally may recheck the CVV2 and return another CVV2 result code or solely rely on the V.I.P. CVV2 results and return the CVV2 result code along with the appropriate response code.

Issuers also may use CVV2 for the following purposes:

- To augment the effectiveness of voice referrals
- For address changes, to prevent account takeover fraud, and for card activation

Issuers can perform their own CVV2 validation, have V.I.P. validate the CVV2 for them, or both. If V.I.P. performs the validation, it verifies the CVV2 before the authorization request is passed to the issuer or to the V.I.P. stand-in processor (STIP). Issuers can choose to have V.I.P. check the CVV2 in all CVV2-eligible authorization requests.

For a comprehensive description of this service, refer to *V.I.P. System Services.*

Other Risk Control Services

The following risk control services are also available for SingleConnect members:

- Fraud Reporting System (FRS)
- Automatic Cardholder Database (Auto-CDB) Update
- Cardholder Risk Identification Service (CRIS)
- International Automated Referral Service (IARS)

These services are described in the following sections. In addition, the Visa Smart Debit and Visa Smart Credit (VSDC) product, which provides additional risk control features, is briefly described in Chapter 1, Service Overview.

Online Fraud Reporting Service

The online fraud reporting capability is optional and allows members to report fraud transactions using online messages. Fraud notifications can also be sent through the BackOffice Adjustment System (BOAS).

Acquirers are required to report fraud activity when the acquirer determines that the issuer did not exist at the time of the transactions, the account number fails a modulus-10 check digit test, or because of other situations as discussed in the Visa Operating Regulations. Issuers must report all confirmed fraud activity. Failure to comply with the fraud reporting rules as defined in the Visa Operating Regulations can result in the loss of chargeback rights and potential fines and penalties.

SingleConnect issuers and acquirers use 9620 advices to report confirmed fraud transactions. SMS holds these requests until end-of-day processing when they are forwarded to the Fraud Reporting System. When SMS receives a 9620 advice from the member, it generates a 9630 response.

The following fields are key Fraud Reporting message fields:

- Field 63.9—Fraud Data. This field is mandatory in 9620 advices and identifies the type of fraud being reported. It also designates whether the transaction is being added, modified, or deleted in the Fraud Transaction File.
- Field 70—Network Management Information Code. Acquirers use a value of 940. Issuers use a value of 941.
- Field 125, Usage 3—Reporting Non-NRI/ICS Individual Fraud Transactions. This field usage contains further information about the fraud transaction. Information includes the type of fraud notification, whether the transaction was authorized, a fraud reporting sequence number, the postal code, and fraud investigative status.

For more information, refer to the *Fraud Reporting System User's Guide*.

Automatic Cardholder Database (Auto-CDB) Update Service

Auto-CDB Update service is a real-time service that monitors accounts receiving Pick-Up Card responses and adds them to the Exception File with Pick-Up Card status automatically. Participation in Auto-CDB is optional.

The following messages apply:

- 0210 Financial Transaction Response—When issuers specify the pickup action code (04, 07, 41, or 43) in field 39 and the account is not already listed on the Exception File with a pickup status, SMS updates the Exception File and sends an 0322 advice.
- 0322 File Update Advice—This message notifies the issuer that the Exception File was updated; it includes all information in the updated exception record. A value of 9030 in Field 63.4—STIP/Switch Reason Code indicates an Auto-CDB advice.
- Field 91—File Update Code (with a value of 1, 2, 3, or 5) also appears in the 0322 advice and must not contain the value 4. It is not returned in 0332 responses.
- 0332 File Update Advice Response—Issuers must generate an 0332 response to acknowledge receipt of the 0322 advice.

Cardholder Risk Identification Service (CRIS)

Visa's CRIS is an innovative transaction scoring and reporting service that employs neural network technologies to develop risk scoring models that identify fraudulent transaction patterns. Issuers can use CRIS as a stand-alone fraud detection system or as a complement to their internal fraud detection methods.

The CRIS system scans the V.I.P. System log files and a brief history of transactions of each cardholder to examine approximately 80 different criteria to determine the risk level of each authorization. The alert process notifies issuers of transactions with the highest probability of fraud. These alerts are then electronically sent to issuers throughout the day for further investigation.

The CRIS System can deliver alerts to issuers as reports sent through public networks such as CompuServe and G.E. Information Services or online as advice messages through VisaNet. All of these methods are available to SingleConnect issuers.

For alerts delivered online, CRIS sends a file of alerts to VisaNet up to 144 times a day. VisaNet formats the alerts into 0620 Administrative Advice Messages and places them in the issuers' advice message files. The issuers may recover these alerts at any time.

Issuers acknowledge receipt of the advices by responding with 0630 Administrative Advice Response Messages. The 0630 response messages are matched to their corresponding 0620 CRIS alert messages.

Key fields in these advices are:

- Field 48—Additional Data, Private, usage 29 (CRIS Alert, Part 1), which contains the CRIS alert type and the CRIS transaction risk score.
- Field 70—Network Management Information Code, which contains a

value of 0174 to identify the message as a CRIS alert.

- Field 125—Supporting Information, usage 1 (CRIS Alert, Part 2) contains additional data, such as an indication of whether or not the original transaction passed the CVV check.

Issuers interested in subscribing to CRIS or current CRIS subscribers who wish to receive their alerts online should contact their Visa representative.

International Automated Referral Service (IARS)

IARS, which is mandatory for Visa POS acquirers and issuers that process international referrals, helps to reduce the problem of lost sales caused by unanswered referrals. Visa provides the capability of stand-in processing and advice creation for SMS issuers for transactions acted upon by IARS. It improves referral handling for Visa members, cardholders, and merchants worldwide by:

- Providing a faster referral process and a guaranteed response to referral calls, thereby enhancing Visa service quality to merchants and Visa cardholders.
- Increasing the cost-effectiveness of referrals as a fraud prevention tool.

When a referral response to an authorization request is received at the point of sale, the merchant contacts the acquirer. The acquirer may confirm that the issuer or VisaNet system has generated a referral by submitting another authorization request. If the referral is confirmed (a code of “01” or “02”—refer to card issuer—in field 39 of the 0110 response), the acquirer then dials one number for all issuers. The IARS will attempt to route the call to the issuer. If the issuer does not respond, the call is handled according to IARS stand-in procedures, either through the Voice Response Unit (VRU) or a Referral Center Agent.

If the issuer does not respond, an advice (0120) will be generated for the issuer to recover.

The key fields in this advice are:

- Field 38—Authorization Identification Response, which ends in:

  X = authorization decision by the Visa Referral Center.

  R = authorization decision by the IARS Voice Response Unit (VRU).

- Field 44.1—Response Source/Reason Code, which contains:

  9 = the advice was generated by IARS.

  4 (issuer unavailable for processing) = issuer is not certified to receive code 9.

- Field 63.4—STIP/Response Reason Code, which contains:

  9029 = the authorization was approved in stand-in by the VRU or referral center

  9011 = the authorization was approved in stand-in by the VRU or referral center however the member was not certified
  (the line to issuer is down)

Issuers or acquirers interested in subscribing to IARS should contact their Visa representative.

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.

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.

Security considerations not directly related to financial transaction interchange are beyond the scope of this document.

Visa Smart Debit and Visa Smart Credit (VSDC) offline PIN is not included in this chapter. Details can be found in:

- The Visa Smart Debit and Credit Planning Guide
- The Visa Smart Debit and Credit Member Implementation Guide

In addition to the applicable SingleConnect bylaws and operating regulations, SMS participants are also governed by the security standards and requirements in:

- *Consolidated PIN Security Standards Requirements.*
- *Card Technology Standards Manual.*

This chapter reflects the information in the *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. For help getting copies of the security manuals and related information, contact your Visa representative.

Visa and Visa Electron PIN Usage

PINs are conditional on Visa and Visa Electron purchase transactions. Although the majority of Visa and Visa Electron transactions currently do not include the cardholder's encrypted PIN, some transactions include the PIN.

Visa and Visa Electron issuers must make a PIN available to each cardholder. The issuer's card acceptance policies, including PIN requirements, are communicated to the point-of-sale (POS) device by reading the extended service codes encoded on the magnetic stripe data. Values relating to PINs are located in the third position of the Service Code field. For information about specific service codes, refer to the *Card Technology Standards Manual*.

The use of the extended service code is optional for Visa issuers. Although Visa's operating rules do not currently require acquirers to act upon the service code for PIN requirements, some acquirers have begun using the service code to determine if a PIN should be included.

Visa and Visa Electron acquirers supporting Automated Dispensing Machine (ADM) devices must accept PINs and, by prompting for the PIN, the merchant can reduce possible chargebacks. An ADM is an unattended terminal that accepts payment for dispensing goods (such as fuel), has electronic capability, and accepts PINs, but does not disburse currency.

Issuers must be prepared to receive and process the encrypted PIN on authorizations (0100) and full financials (0200). Acquirers need to determine if their merchants should support PIN processing. Both issuers and acquirers need to follow the standards discussed in this chapter to ensure the security of the PIN.

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 is dependent 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 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 devices belonging to other institutions or controlled by other networks and service providers.

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 also are 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 in accordance with 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* only be placed in service if there are assurances that the equipment has not been subject to unauthorized modifications or tampering.

Once TRSMs are placed in service, at a minimum, the following procedures and controls *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 that had been 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* only be placed in service 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, reencryption, 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 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 reissuing 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 POS 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 such that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys by using statistical randomness.

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.

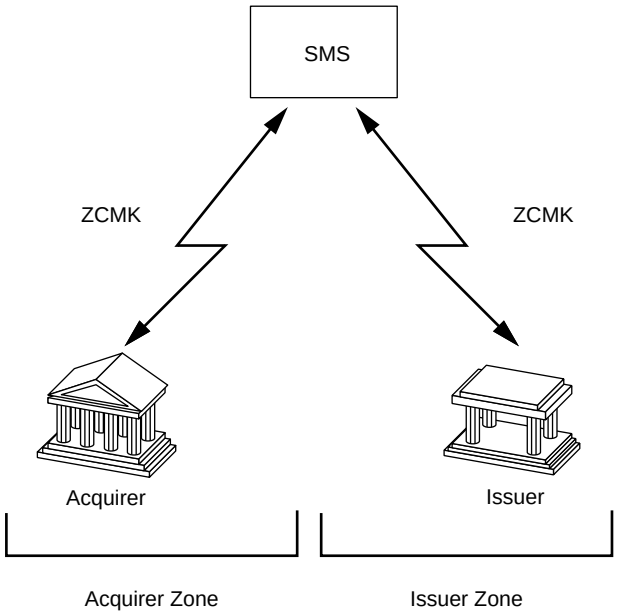
PIN processing in a DES-based zone encryption scheme is characterized by two zones: an acquirer zone and an issuer zone. SMS is a participant in each of these zones and functions as a cryptographic intermediary.

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 having 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 by transferring 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, 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, the destruction of keys *must* be observed 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 include 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

SingleConnect 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 the injecting 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, 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 8–1SMS Transaction Routing (1 of 2)

Transaction	Message Type	Routing Decision Based on...
Authorization (Visa and Visa Electron)	0100	The account number contained in Field 2—Primary Account Number
Purchase (SMS POS), Merchandise Return	0200	
Cash Disbursement	0200	
Reversal	0420	
Adjustment, Representment	0220	
Chargeback, Chargeback Reversal Issuer-initiated Fee Collection/Funds Disbursement	0422	The acquirer ID contained in Field 32—Acquiring Institution Identification Code.
Acquirer-initiated Fee Collection/Funds Disbursement	0220	The issuer ID contained in Field 100—Receiving Institution Identification Code or in Field 2—Primary Account Number. (Field 100 takes priority over field 2 if both fields are provided.)
Text Messages	0600	The member identified in Field 100—Receiving Institution Identification Code.
Copy Requests	0600	The acquirer ID contained in Field 32—Acquiring Institution Identification Code.
Copy Confirmations	0600	The account number contained in Field 2—Primary Account Number.
CRIS Alerts	0620	The issuer identified in Field 100—Receiving Institution Identification Code.

Table 8–1SMS Transaction Routing (2 of 2)

Transaction	Message Type	Routing Decision Based on...
Fraud Notifications	9620	The issuer identified in Field 100—Receiving Institution Identification Code.

Routing Options, Tables, and Services

Routing options are determined by issuers and acquirers. This section discusses the relationship between SMS POS products and the following items:

- Routing tables
- Priority Routing Service
- Alternate Routing Service
- Split Routing Service

Gateway Services also are available to SMS acquirers. 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 using the same connections used for Visa transactions. For more information, see the *V.I.P. System Services* manual.

Routing Options

The Routing Service options for Visa and Visa Electron are shown in Table 8–2.

Table 8–2: Visa and Visa Electron Routing Table and Service Options

Routing Service	Acquirer	Issuer
Routing Tables	Optional	
Priority Routing	Optional	
Alternate Routing	Optional	Optional
Split Routing		Optional

Routing Tables

This subsection discusses the routing tables that apply to each SMS product.

Visa Routing Table

The Visa Routing Table is a batch data file, created weekly, that lists all Visa card prefixes, prefix lengths, and account number lengths. The table helps Visa acquirers make authorization routing decisions.

This table is optional.

Visa Electron Routing Table

The Visa Electron Routing Table is a batch data file, created weekly, that lists all Visa Electron card prefixes, prefix lengths, and account number lengths. The table helps Visa Electron acquirers make authorization routing decisions.

This table is optional.

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 authorizations, 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, 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:

- Adjustments and back office adjustments.
- Chargebacks.
- Chargeback reversals.
- Representments.
- Fee-related transactions.
- Administrative messages, including:
  - Free text.
  - Copy request and confirmation messages.
- Fraud notification messages.
- Updates to the Exception File, PIN Verification File, or both.

Only issuers or their designates can update the Exception, PIN Verification, and Address Verification files.

For exception transactions, fee-related transactions, and administrative messages, different endpoints can be specified for POS transactions. An alternate endpoint can be used for POS 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 POS transactions.

Alternately routed transactions can be settled at an alternate settlement entity. An alternate settlement entity can only be specified for alternately routed transactions.

Split Routing

The Split Routing Service allows issuers to separate types of transactions and to route these transactions to two or more issuer processing centers. The service offers three routing options, PIN/No-PIN, ATM/POS, and ATM Account Type.

POS PIN/No-PIN Split Routing—This option is available for SMS issuers that process Visa and Visa Electron POS transactions, and ATM transactions. Issuers may use this option when their own card processing center does not have the ability to verify PINs in a secure environment. Issuers can designate one processor to receive all PIN-based transactions and another processor to receive transactions not requiring a PIN.

ATM/POS Split Routing—This option is available for SMS issuers that process Visa and Visa Electron POS transactions, and ATM transactions. It allows issuers to use separate processing centers for ATM transactions and for POS 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:
  - Purchases
  - Cash disbursements
  - Reversals of purchases
  - Reversals of cash disbursements
  - 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.

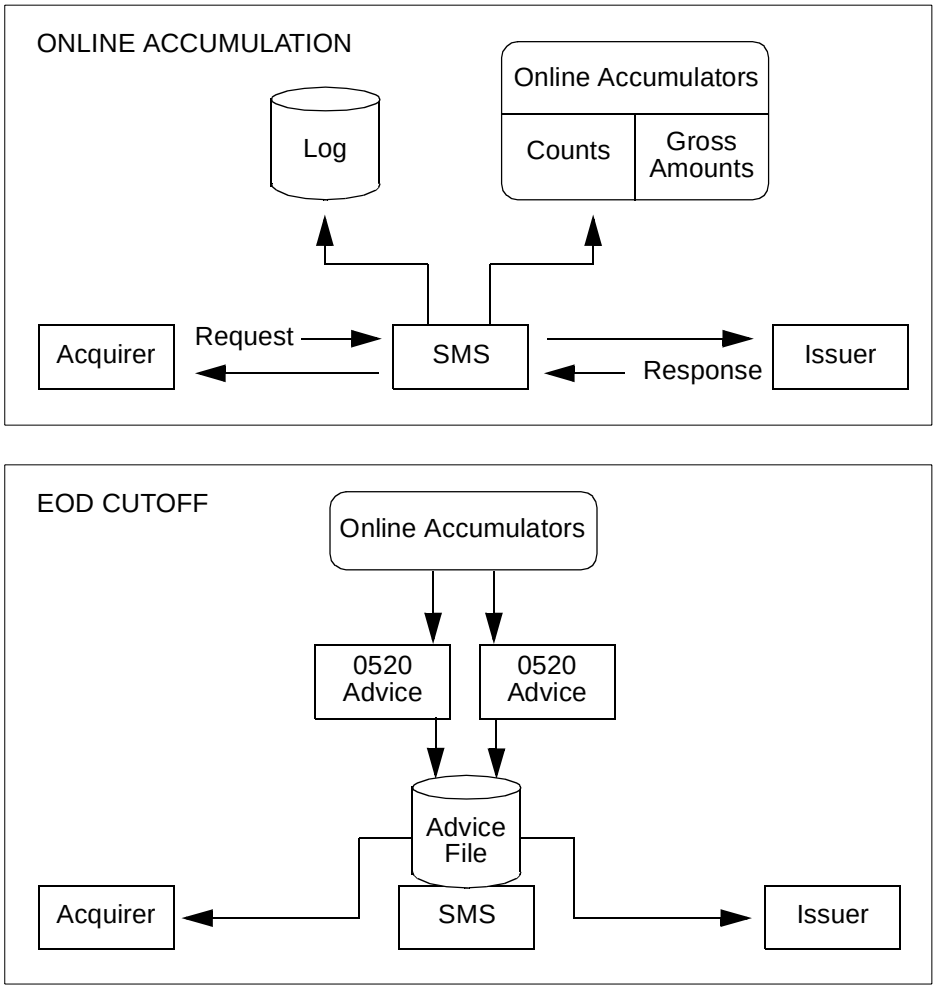
In addition, members can request 0500 reconciliation advices that contain the cumulative settlement totals for the day, from start of processing to the time of the request for the advice.

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)

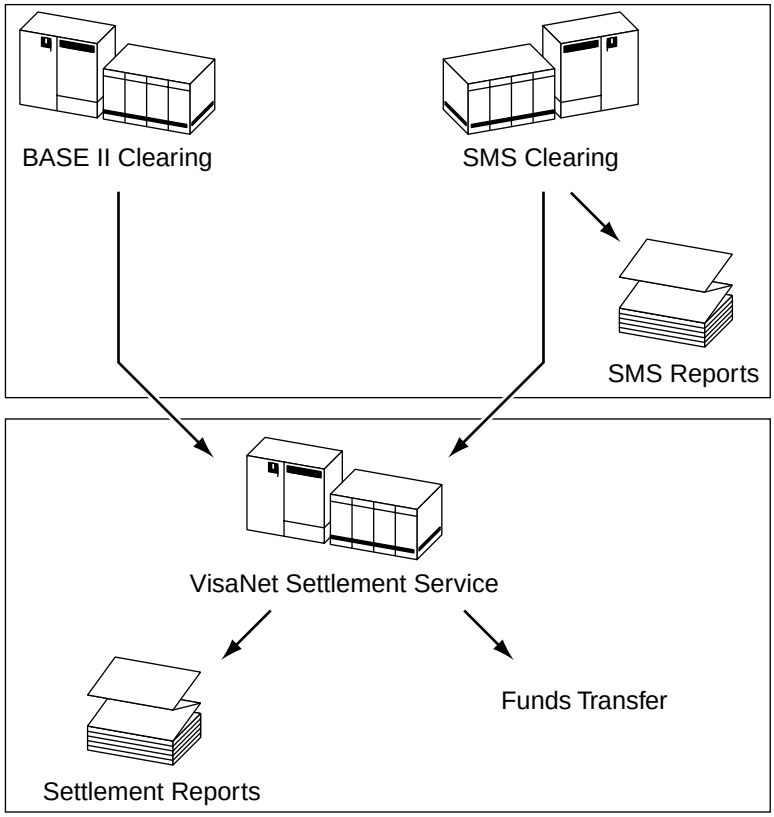
SingleConnect members settle through VSS. Visa processes interchange transactions for SMS and BASE II through separate systems. Both SMS and BASE II perform their own clearing functions. VSS performs the settlement functions for SMS and BASE II in one centralized service that ensures consistency in settlement 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—Visa and Visa Electron Transactions

GMT Dates	GMT
First Sunday in April to last Sunday in October	0500
Last Sunday in October to first Sunday in April	0600

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:

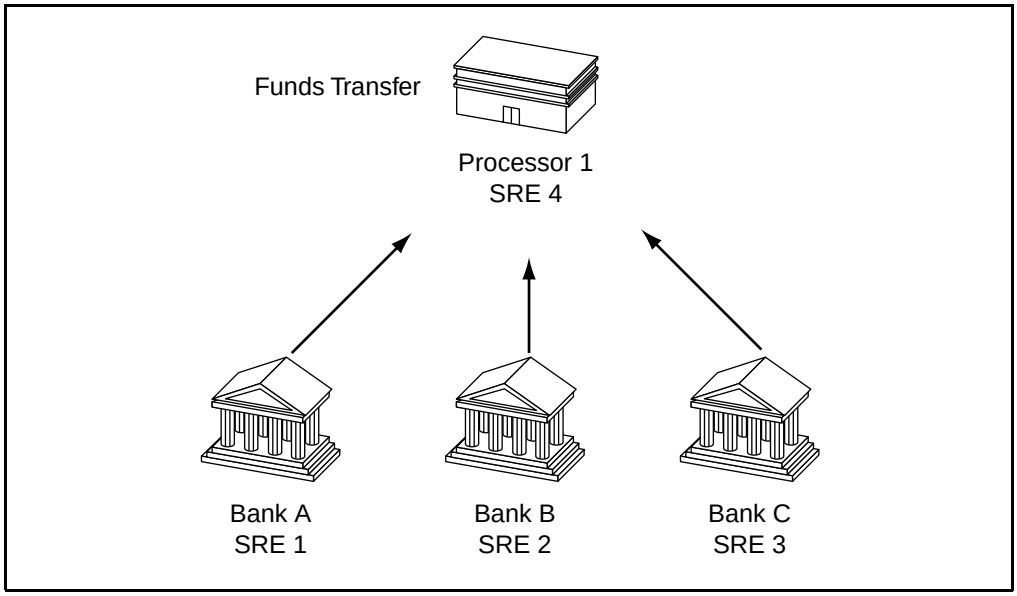
- Processor performs funds transfer for all members.
- Processor performs funds transfer for some members and not others.
- Processor supports National Net Settlement Service transactions.

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.

Member-to-Visa Connection Options 10

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 POS (Visa & Visa Electron) 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 10–1.

Table 10–1: VAP File Types

File Name and Description	File Type (VAP Pullkey)	TC Records Used For Data Records or Printlines
Undifferentiated • Visa Routing Table • 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
BASE II Deferred Clearing Advices ISO-formatted or fixed-format clearing advices from dual-message acquirers to single-message issuers. **Note:** Fixed format available only through Deferred Clearing Advice File (DCAF). DCAF supports ISO-formatted advices and fixed-format advices. See Chapter 11, Considerations for Issuers.	ISO or FIXED	0220 bit-mapped full financial messages Fixed-format full financial messages
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.

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.
- Receive deferred clearing draft transactions through bulk retrieval. For more information on receiving deferred clearing advices in bulk files, see the Deferred Clearing Advice File (DCAF) Service section in Chapter 1, Service Overview.

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 end of day, members' VAPs receive settlement and reconciliation reports from VisaNet.

A member may want to receive its SingleConnect reports, 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. In 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 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 in this manual.

Considerations for Issuers 11

This chapter is intended for SingleConnect members that issue Visa or Visa Electron cards.

Visa and Visa Electron acquirers can choose to submit transactions using the single-message or dual-message mode. In the dual-message mode, the acquirer sends above floor limit POS transactions made with a Visa or Visa Electron card as authorization requests (0100). One to several days later, the acquirer submits BASE II deferred clearing records (TC 05 and TC 06). SMS clears these records to the SingleConnect issuer as deferred clearing advices (0220s), messages similar to the online deferred clearing advices described in Chapter 4, Message Types and Flows.

As a result, Visa and Electron issuers that choose to connect to Visa's Single Message System (SMS) must be prepared to receive both online financial transactions from single-message acquirers and authorization messages followed by deferred clearing transactions from both single-message and dual-message acquirers.

The net effect is that, for POS transactions acquired in dual-message mode, the issuer must be prepared to accept authorization requests (0100), which have no financial impact. The issuer may choose to manage the cardholder's available balance or credit line by placing a temporary hold on funds until the 0220 advice is received. Since there could be circumstances where the 0220 advice is not received (for example, a reversal was not properly processed), the issuer may wish to establish an expiration date for holds, possibly three to four days after the authorization date.

Another consideration for SingleConnect issuers is that, for cross-currency transactions from dual-message acquirers, the cardholder billing amount on the 0220 may be different from the amount authorized. This may be due to fluctuations in currency conversion rates between the date of the authorization and the date the transaction clears.

Issuers also need to remember that acquirers may not know the final amount at the time of authorization and that some transactions may not have required an authorization since they were below a floor limit.

Basic Transaction Flows

This section illustrates two basic transaction flows to SingleConnect issuers. The flows describe both a deferred clearing transaction originated at a SingleConnect acquirer (Figure 11–1) and a dual-message acquirer (Figure 11–2). In both examples, the advice may be received one to several days after the authorization.

Figure 11–1: SingleConnect Acquirer and Issuer: Online Deferred Clearing Transaction

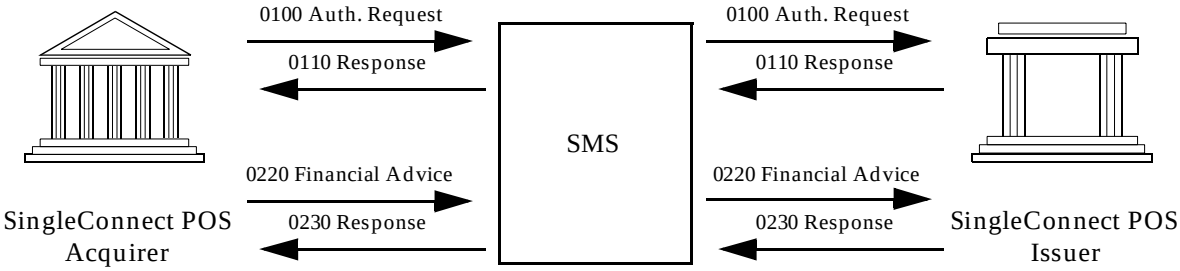
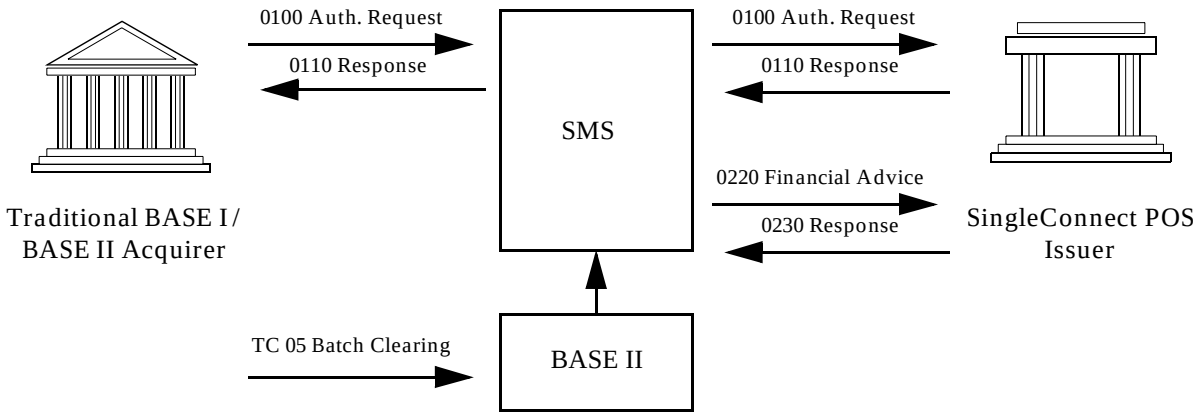


Figure 11–2: Dual-Message Acquirer and SingleConnect Issuer: BASE II Deferred Clearing Transaction (Delivered to Issuer as Online Deferred Clearing Transaction)



The following sections highlight the areas where the SingleConnect issuer of VISA or Electron cards needs to consider the effect of POS transactions acquired in dual-message mode:

- Multicurrency Support Considerations
- Connectivity and Deferred Clearing Advice Retrieval
- Deferred Clearing and Settlement Considerations
- Repeat Message Considerations
- Additional Message Formats

Multicurrency Support Considerations

For cross-currency transactions from dual-message acquirers, the cardholder billing amount can be different from the amount authorized. This difference is due to fluctuations in currency conversion rates between the date of the authorization and the date the transaction clears.

IMPORTANT

The transaction amount in the transaction currency is consistent in the authorization and clearing records. This value is the amount that should be quoted to cardholders until the clearing transaction is settled and the final billing amount is posted to the cardholder's account.

For more information, refer to Chapter 5, Multicurrency Support.

Connectivity and Deferred Clearing Advice Retrieval

An issuer can connect to VisaNet through:

- A VisaNet Access Point (VAP) using different types of VAP stations:
  - Stations for online message processing and advice recovery from the Online Advice File.
  - Stations for file transfer.
  - Test stations.

  For more information on VAP configurations, refer to Chapter 10, Member-to-Visa Connection Options. Also refer to *VAP Interface Specifications: BASE II and Other File Processing*, and *VAP Interface Specifications: V.I.P. Processing*.

A SingleConnect issuer receives transactions as BASE II deferred clearing advices (0220s) when the transactions are acquired in dual-message mode. Issuers select one of the following methods for retrieval of BASE II deferred clearing advices:

- Online Advice Retrieval from one station. This process retrieves advices from the online advice file by using a single online station.
- Online Advice Retrieval from multiple stations. This process retrieves advices from the online advice file using more than one online station.
- DCAF retrievals. SMS issuers can use the DCAF Service to retrieve deferred clearing advices in bulk files through a separate network connection. At the issuer's option, bulk files are delivered in ISO format or DCAF fixed format. For more information about this service, refer to "Deferred Clearing Advice File (DCAF) Service" in Chapter 1, Service Overview.

The SMS Advice Retrieval Service allows issuers to recover their stand-in processing (STIP) advice data from the SMS Advice File. For details about this service, including one-station and multiple-station retrievals from the SMS Advice File, refer to *V.I.P. System Services*.

For information about SMS Advice File retrievals, see Chapter 6, Stand-In and Card Verification Value Processing.

The VAP configuration should be customized to the member's environment and future plans. For configuration assistance, contact your Visa representative.

Deferred Clearing and Settlement Considerations

The clearing and settlement of transactions acquired by a dual-message (BASE II) acquirer may occur several days after the authorization.

As stated earlier in this chapter, the SingleConnect issuer chooses how to receive the dual-message-acquired (BASE II) deferred clearing advices. There are several other aspects of processing these advices that need to be taken into consideration, particularly when the issuer builds reconciliation procedures. This section discusses the following:

- How to identify (BASE II) deferred clearing advices on reports and raw data
- How to use reconciliation messages
- How to adapt an automated reconciliation tool
- Where exceptions from dual-message acquirers are processed

Identification of BASE II Deferred Clearing Advices

BASE II deferred clearing transactions can be identified in two ways:

- Field 10—Batch Number in the message header contains a value of 255

  U.S. members can identify CRS exception transactions with a value of 100 in Field 10—Batch Number of the header. These transactions also have a value of 9101 in Field 63.4

- Field 63.4—STIP/Switch Reason Code contains a value of 9100 or 9101

  Note that a value of 9101 and 9100 can appear in raw data although only a value of 9101 appears in the V.I.P. online message. Issuers should treat the values as equals.

DS transaction detail reports include both of the above fields as part of the information provided on each transaction.

In addition, the V21200 record of raw data contains the batch number, and the V21210 record contains the STIP/Switch Reason Code.

If a BASE II deferred clearing advice for a transaction that occurred on a previous day is being researched, Field 15—Settlement Date always contains the settlement date of the DS detail report on which the transaction appears.

Reconciliation Messages and V.I.P. Message Consideration

BASE II deferred clearing advices are not included in the totals provided by the online reconciliation messages (0500 or 0520). These transactions are identified with a STIP/Switch Reason Code of 9101. A value of 9100 is always converted to a value of 9101 in V.I.P. messages.

Automated Reconciliation Considerations

The issuer that elects to receive BASE II deferred clearing transactions receives them on the day after the transactions are settled.

The net effect is that the raw data file contains transactions with multiple settlement dates. For example, the SMS raw data file includes:

- Purchases and merchandise returns from SingleConnect acquirers with a settlement date of September 23.
- BASE II deferred clearing advices with a settlement date of September 23.

The issuer's internal log for the same period of time includes:

- Purchases and merchandise returns from SingleConnect acquirers with a settlement date of September 23.
- BASE II deferred clearing advices with a settlement date of September 22.

Exceptions from Dual-Message Acquirers

Exceptions from dual-message acquirers are distributed in the same manner as exceptions from SingleConnect acquirers. SMS routes representments, funds disbursements, and free text messages from a dual-message acquirer to the issuer or the alternate routing destination requested by the issuer.

Repeat Message Considerations

Repeat messages can be used by BASE I acquirers when a transaction times out. SingleConnect issuers can thereby receive both authorization messages and reversal messages from acquirers connected to the BASE I system. SingleConnect issuers must be able to recognize and process a repeat message.

BASE I acquirers identify a repeat message by changing the Message Type from an 0100 to an 0101 for authorization requests and from an 0400 to an 0401 for reversal requests. Every field in the message, including the fields in the message header, must remain unchanged, although there are some instances where Field 7—Transmission Date and Time may also be changed. If STIP processes a repeat request, issuers receive an 0121 advice or an 0421 advice.

SingleConnect acquirers must always send a reversal if a transaction times out. Repeat messages are not used by SingleConnect acquirers.

NOTE: *This document does not routinely show repeat or repeat advice messages. Assume that the message/fields requirements for a repeat (0101, 0401) are the same as the corresponding original (0100, 0400) and a repeat advice (0121, 0421) are the same as the corresponding advice (0120, 0420).*

Additional Message Formats

Message formats from dual-message acquirers are identified as BASE II advices and are included in message formats chapter of the of the *V.I.P. System SingleConnect Service POS (Visa & Visa Electron), Technical Specifications, Volume 2*.

Visa Secure Electronic Commerce A

Visa Secure Electronic Commerce (VSEC) provides a secure method of payment using credit or debit cards over open networks. VSEC is supported by the SET Secure Electronic Transaction™ Protocol, which is a secure bankcard processing method developed jointly by Visa, MasterCard, and other companies. VSEC transactions can be processed through SMS as dual message or single message POS transactions.

VSEC SMS Message Types

The SMS message types valid for VSEC processing are:

- 0100 authorizations and 0120 authorization advices
- 0200 financials and 0220 financial advices
- 0200 adjustments and 0220 adjustment advices
- 0200 merchandise credits and 0220 merchandise credit advices
- 0400 authorization or financial reversals and 0420 reversal advices
- 0422 chargebacks and 0480 chargeback status advices
- 0422 chargeback reversals and 0480 chargeback reversal status advices
- 0220 representments and 0282 representment status advices
- 9620 fraud advices

Key Fields

The key fields used to distinguish a VSEC authorization or financial message from non-VSEC messages are shown in Table A–1.

Table A–1: Valid VSEC Message Types

Messages	Field 25—POS Condition Code	Field 60, Positions 9–10, Electronic Commerce Indicator	Field 63.6, Position 4, Mail/ Telephone or Electronic Commerce Indicator	VSEC Fields 126.6–126.9
0100 authorization requests	✔	✔		✔
0400 authorization reversals and their advices	✔	✔		
0200 financial requests	✔		✔	✔
0400 financial reversals and their advices	✔		✔	
0200 adjustments and 0220 adjustment advices			✔	
0200 merchandise credits and 0220 merchandise credit advices	✔		✔	
0422 chargebacks and 0480 chargeback status advices			✔	
0422 chargeback reversals and 0480 chargeback reversal status advices			✔	
0220 representments and 0282 representment status advices			✔	
9620 fraud advices			✔	

Field 25—POS Condition Code

Field 25 signifies that the transaction is a VSEC request when it contains code 59. Certified issuers receive the 59. For noncertified issuers, V.I.P. replaces the 59 with 08, which indicates a Mail Order/Telephone Order (MOTO).
Field 25 is returned in responses. It is required in authorization requests and reversals and their advices. It also is required in financial requests, their reversals and their advices as well as in merchandise credits and advices.

Field 60, Positions 9-10, Electronic Commerce Indicator

Positions 9 and 10 of Field 60—Additional POS Information contain a 2-digit code indicating the level of security used in a VSEC transaction over an open network. This field is supplied by acquirers and is required in authorization requests, authorization reversals and their advices. It is not returned in responses. The subfield values are:

00 = Not applicable

05 = Secure Electronic Transaction with cardholder certificate

06 = Secure Electronic Transaction without cardholder certificate

07 = Channel-encrypted electronic commerce transaction

08 = Nonsecure electronic commerce transaction

The V.I.P. System drops the subfield if the issuer is not certified to receive it.

Field 63.6, Position 4, Mail/Telephone or Electronic Commerce Indicator

Position 4, of Field 63.6—Chargeback Reduction/BASE II Flags, indicates the level of security of an electronic commerce transaction. It is required in financial requests and reversals, adjustments, merchandise credits, chargebacks, chargeback reversals as well as their related advices. It also is required in fraud advices. It is not returned in response messages. Allowable electronic commerce values are:

5 = Secure Electronic Transaction with cardholder certificate

6 = Secure Electronic Transaction without cardholder certificate

7 = Channel-encrypted electronic commerce transaction

8 = Nonsecure electronic commerce transaction

Field 63.6, position 4, is a retain-and-return field. Exception transactions must have the same value as in the original financial transaction.

Field 126.6—Cardholder Certificate Serial Number (VSEC)

Field 126.6 is a value assigned to a SET™ cardholder certificate issued by the issuer's certificate authority. The number's specific size and data type is not defined by the SET standard.

This field appears in an 0100 authorization request or 0200 financial request if it represents a SET transaction.

If the cardholder certificate does not appear in the SET transaction, this field must not be sent.

Field 126.7—Merchant Certificate Serial Number (VSEC)

Field 126.7 is a value assigned to a SET merchant certificate issued by the acquirer's certificate authority. The number's specific size and data type are not defined by the SET standard.

This field appears in an 0100 authorization request or 0200 financial request if it represents a SET transaction. It is not returned in 0110 or 0210 responses.

Field 126.8—Transaction ID (VSEC)

The VSEC transaction ID is a unique number generated by the merchant server to identify the transaction. This ID is part of the TransStain (field 126.9).

This field appears in an 0100 authorization request or 0200 financial request if it represents a SET transaction. It is not returned in 0110 or 0210 responses.

Field 126.9—TransStain (VSEC)

The TransStain is a 20-byte hash value calculated by applying a secure hash algorithm to the Transaction ID and CardSecret.

- The TransStain proves the presence of the cardholder certificate in a SET transaction.
- A CardSecret is a secret SET-defined value known only to the cardholder and the issuer of the cardholder certificate.

The TransStain cannot be reproduced or copied from one transaction to another. If no cardholder certificate is present in the transaction, the TransStain is calculated using a CardSecret of zeros.

This field appears in an 0100 authorization request or 0200 financial request if it represents a SET transaction. It is not returned in 0110 or 0210 responses.

Index

A

B

C

D

E

F

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

Z