Welcome to V.I.P. System Overview

The *V.I.P. System Overview* has been updated. This manual contains a high-level, general overview of the VisaNet Integrated Payment (V.I.P.) System and its components, files, processes, and services. The manual describes *VisaNet* (Visa's transaction processing network) and illustrates how the V.I.P. System fits into the network.

V.I.P. System Overview contains updated service descriptions for services available through the V.I.P. System.

This book is part of the suite of V.I.P. System documents. *V.I.P. System Overview* is designed to be a companion to *V.I.P. System Services, Volume 1 and Volume 2*, which has also been updated. The two manuals incorporate all of the system changes and revisions described in VisaNet Business Enhancements technical letters published after April 2003 through April 2004. Refer to About This Manual for a complete list of information sources used to prepare this *V.I.P. System Overview* manual. It directs readers to sources for more detailed information.

The Visa *Confidential* label indicates that 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.

Please send questions or comments to Docline@visa.com.

Effective: 30 June 2004

© Visa International 2000, 2002, 2003, 2004

THIS PAGE INTENTIONALLY LEFT BLANK.

V.I.P. System Overview

V.I.P. SYSTEM

Effective: 30 June 2004

© Visa International 2000, 2002, 2003, 2004

THIS PAGE INTENTIONALLY LEFT BLANK.

Contents

About This Manual....1

Audience....1

Organization of This Manual....1

Document Conventions....1

V.I.P. System Documentation Descriptions....2

Sources of V.I.P. Information....6

Obtaining Report Samples....7

For More Information....7

CHAPTER 1 V.I.P. SYSTEM BASICS

1.1 VisaNet Overview....1-1

1.2 Visa Products....1-2

1.3 VisaNet Components....1-3

1.4 VisaNet Systems....1-5

1.4.1 VisaNet Integrated Payment (V.I.P.) System....1-6

1.4.1.1 BASE I System....1-6

1.4.1.2 Single Message System (SMS)....1-7

1.4.2 BASE II System....1-8

1.4.3 VisaNet Distributed Processing System (VDPS)....1-9

1.4.4 The Common Member Interface (CMI) and Other Access Methods....1-10

1.4.5 VisaNet Settlement Service (VSS)....1-11

1.4.6 V.I.P. Processing Parameters....1-12

1.4.7 V.I.P. Messages....1-13

CHAPTER 2 V.I.P. TRANSACTION PROCESSING

2.1 Transaction Flow....2-1

2.2 V.I.P. Message Processing....2-2

2.3 Message Validation and Preparation....2-2

2.3.1 Message Formats....2-3

2.3.2 V.I.P. Message Structure....2-3

2.3.3 Message Matching....2-4

2.4 Message Routing Basics....2-4

2.4.1 Routing Messages....2-4

2.4.1.1 System Tables Routing Information....2-5

2.4.1.2 Routing Tables....2-5

2.4.1.3 Internal Routing Services....2-6

2.4.1.4 Gateways to Non-VisaNet Destinations....2-6

2.5 Stand-In Processing (STIP)....2-6

2.5.1 BASE I STIP....2-7

2.5.2 SMS STIP....2-8

Contents

2.6 Response Processing....2-8

2.7 Logging....2-9

2.8 Additional V.I.P. Functions....2-9

2.8.1 Managing the Network....2-9
2.8.2 Managing System Tables....2-9
2.8.3 Managing System Databases....2-10
2.8.3.1 Cardholder Database Files....2-10
2.8.3.2 Merchant Central File....2-12
2.8.4 Reporting....2-12
2.8.4.1 BASE I Reports....2-12
2.8.4.2 Settlement Reports....2-12
2.8.4.3 Raw Data Records....2-13
2.8.5 Billing....2-13

CHAPTER 3 V.I.P. SYSTEM SERVICES

3.1 Service Functional Groups....3-1

3.2 Routing Service Definitions....3-4

3.2.1 ATM/POS Split Routing Service....3-4
3.2.2 Check Acceptance Service....3-4
3.2.3 Gateway Services....3-4
3.2.4 Integrated Debit Service....3-5
3.2.5 PIN/No-PIN Split Routing Service....3-5
3.2.6 Priority Routing Service....3-5
3.2.7 Visa Shortest Online Path (VSOP) Service....3-5

3.3 Routing Service Availability....3-6

3.4 Risk Management Service Definitions....3-6

3.4.1 Card Recovery Bulletin (CRB) Service....3-6
3.4.2 Fraud Reporting System (FRS)....3-7
3.4.3 Visa Issuer Fraud Detection (VIFD) Service....3-7

3.5 Risk Management Service Availability....3-7

3.6 Visa Secure Electronic Commerce (VSEC) Service Definition....3-7

3.6.1 Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)....3-7

3.7 VSEC Service Availability....3-8

3.8 Chip Card Service Definitions....3-8

3.8.1 Visa Cash CEPS Service....3-8
3.8.2 Visa Horizon Service....3-8
3.8.3 Visa Smart Debit/Smart Credit (VSDC) Service....3-8

3.9 Chip Card Service Availability....3-9

3.10 Authorization Database Service Definitions....3-9

3.10.1 Automatic Cardholder Database Update (Auto-CDB) Service....3-9
3.10.2 Merchant Central File Service (MCFS)....3-9

3.11 Authorization Database Service Availability....3-10

3.12 Authorization Service Definitions....3-10

3.12.1 Account Verification Service....3-10
3.12.2 Address Verification Service (AVS)....3-10
3.12.3 Advanced Authorization Service....3-10
3.12.4 Advice Retrieval Service—BASE I....3-11
3.12.5 Advice Retrieval Service—SMS....3-11
3.12.6 ATM Format Conversion Service....3-11
3.12.7 Card Verification Value (CVV) Service....3-11
3.12.8 Card Verification Value 2 (CVV2) Service....3-11
3.12.9 Cardholder Authentication Verification Value (CAVV) Verification Service....3-12
3.12.10 Custom Payment Service (CPS)/ATM....3-12
3.12.11 Custom Payment Service (CPS)/POS....3-12
3.12.12 Deferred Clearing Advice File (DCAF) Service....3-12
3.12.13 Dynamic Key Exchange (DKE) Service....3-13
3.12.14 Full Authorization Service....3-13
3.12.15 International Automated Referral Service (IARS)....3-13
3.12.16 Multicurrency Service....3-13
3.12.17 PIN Verification Service (PVS)....3-13
3.12.18 POS Check Service....3-13
3.12.19 Positive Authorization Capacity Management (PACM) Service....3-13
3.12.20 Positive Cardholder Authorization Service (PCAS)....3-14
3.12.21 Preauthorized Payment Cancellation Service (PPCS)....3-14
3.12.22 Status Check Service....3-14
3.12.23 Visa Cashback Service....3-14
3.12.24 VisaPhone Service....3-15

3.13 Authorization Service Availability....3-15

3.14 Additional Service Definitions....3-16
3.14.1 Chargeback Reduction Service (CRS)....3-16
3.14.2 Visa Check Card II....3-16
3.14.3 ATM Processing Integration....3-16

3.15 Additional Service Availability....3-16

CHAPTER 4 ACQUIRER AND ISSUER RESPONSIBILITIES

4.1 Establishing Processing Centers....4-1
4.1.1 Network Stations....4-1
4.1.2 V.I.P. Message Support....4-1
4.1.3 Testing and Certification....4-2
4.1.4 Network Management....4-2
4.1.5 SMS Reconciliation and Settlement....4-2

4.2 Acquirer Processing Center Requirements....4-3
4.2.1 POS Connections and Procedures....4-3
4.2.2 PIN Security....4-4
4.2.3 Response Procedures....4-4
4.2.4 Merchant Central File Management....4-5
4.2.5 Follow-Up Procedures and Processing....4-5
4.2.6 Other Responsibilities....4-5

4.3 Issuer Processing Center Requirements....4-6

4.3.1 Transaction Authorization....4-6
4.3.2 Cardholder Database Management....4-6
4.3.3 PIN Security....4-6
4.3.4 Coordination With Visa....4-7
4.3.5 Response Procedures....4-7
4.3.6 Follow-Up Procedures and Processing....4-7
4.3.7 Other Responsibilities....4-8

APPENDIX A TRANSACTION TYPES

A.1 Cardholder Transactions....A-2
A.2 Merchant-Authorized Transactions....A-4
A.3 System-Generated Transactions....A-4
A.4 Exception Transactions....A-5
A.5 Fee-Related Transactions....A-5
A.6 Reconciliation Transactions....A-5
A.7 File Maintenance Transactions....A-5
A.8 Administrative Transactions....A-6
A.9 Network Management Transactions....A-6

Index

Figures

1-1 The VisaNet Communications Network....1-4
1-2 VisaNet Communication Flows....1-5
1-3 VisaNet Systems and Transaction Processing....1-6
1-4 The VisaNet Software System Components....1-9
1-5 VIP System Software at the VIC and at the Processing Center....1-11
1-6 VisaNet Settlement Service (VSS) Process....1-12
2-1 VisaNet Basic Process Flow....2-1

THIS PAGE INTENTIONALLY LEFT BLANK.

Tables

1 Document Conventions....2
2 Descriptions of V.I.P. System Manuals....3
1-1 Comparison of Visa Products....1-3
2-1 V.I.P. Message Structure....2-3
3-1 V.I.P. Services by Functional Group....3-1
3-2 Routing Service Availability....3-6
3-3 Risk Management Service Availability....3-7
3-4 VSEC Service Availability....3-8
3-5 Chip Card Service Availability....3-9
3-6 Authorization Database Service Availability....3-10
3-7 Authorization Service Availability....3-15
3-8 Additional Service Availability....3-17
A-1 V.I.P. Transaction Types....A-1

THIS PAGE INTENTIONALLY LEFT BLANK.

About This Manual

The *V.I.P. System Overview* presents general information about the VisaNet Integrated Payment (V.I.P.) System, Visa's main transaction processing system. It describes *VisaNet* (Visa's transaction processing network), defines its hardware and software system components, and explains where the V.I.P. System resides within the network.

This manual also:

- Provides basic information about Visa messages and transactions and gives an overview of V.I.P. transaction processing.
- Lists Visa services available to members connected to the V.I.P. System and provides a brief description of each service.
- Outlines the responsibilities of Visa acquirers and issuers and includes considerations to take into account when deciding to connect to VisaNet.

For specific topics by chapter, see the "Organization of This Manual" section of this chapter.

AUDIENCE

The *V.I.P. System Overview* is intended for readers who have little or no knowledge of VisaNet, the V.I.P. System, and Visa transaction processing. This manual provides a basic, high-level overview of the network and its systems and refers readers to sources for more information about specific topics.

ORGANIZATION OF THIS MANUAL

The *V.I.P. System Overview* is organized as follows:

Chapter 1, V.I.P. System Basics—Provides an overview of the V.I.P. System, including a description of VisaNet, the basic V.I.P. authorization process flow, and VisaNet components. It identifies and discusses both V.I.P. online and V.I.P. offline functions.

Chapter 2, V.I.P. Transaction Processing—Describes V.I.P. messages and transactions and provides an overview of V.I.P. transaction processing.

Chapter 3, V.I.P. System Services—Lists the services available to members connected to V.I.P. and provides a brief definition of each service. Refer to *V.I.P. System Services, Volume 1 and Volume 2*, for complete service descriptions.

Chapter 4, Acquirer and Issuer Responsibilities—Identifies participation requirements and options both for acquirers and for issuers.

Appendix A, Transaction Types—Lists all valid V.I.P. transaction types and indicates whether the transaction is available for processing under the BASE I System, under the Single Message System (SMS), or under both systems.

DOCUMENT CONVENTIONS

Table 1 shows the document conventions used in this manual.

Table 1 Document Conventions

Document Convention	Purpose in This Guide
boldface	Extra emphasis (stronger than italics).
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.
Shaded illustrations	Systems or procedures that are not directly involved in the process being illustrated in the graphic.
White boxes in flow diagrams	White boxes represent request messages.
Shaded boxes in flow diagrams	Shaded boxes represent response messages.
Dotted line boxes in flow diagrams	Boxes with dotted lines illustrate advice messages.

V.I.P. SYSTEM DOCUMENTATION DESCRIPTIONS

This book is part of the set of V.I.P. System documents. The *V.I.P. System Overview* is designed to be a companion to the two-volume *V.I.P. System Services*, which has also been updated. The two manuals contain new and updated information and incorporate all system changes and revisions described in VisaNet Business Enhancements technical letters and in updates published after April 2003 through April 2004. See the "Sources of V.I.P. Information" section of this chapter for a complete list of sources used to prepare this *V.I.P. System Overview* manual.

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

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

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

This manual contains new and updated information and incorporates all system changes and revisions described in VisaNet Business Enhancements technical letters and updates published after April 2003 through April 2004.

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

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

General Information
V.I.P. System Overview Provides basic descriptions of the VisaNet network and its components, connections, processing concepts, requirements, and options. Contains descriptions of the V.I.P. System, access methods, the BASE I System and the Single Message System, issuer and acquirer responsibilities, and Visa Interchange Center (VIC) operations. Also provides a brief introduction to V.I.P. services. Doc ID 0851-04
V.I.P. System Reports Provides sample reports for V.I.P. System services, BASE I, and Single Message System processing. Doc ID 0852-04
V.I.P. System Services, Volume 1 Provides complete information about V.I.P. System services available to BASE I and to SMS users. Service descriptions include basic information, processing requirements, options, features, key message fields, and message flows. Volume 1 contains the following parts: Part 1: V.I.P. Basics Part 2: Routing Services Part 3: Risk Management Services Part 4: Visa Secure Electronic Commerce (VSEC) Services Part 5: Chip Card Services Doc ID 0853A-04
V.I.P. System Services, Volume 2 Provides complete information about V.I.P. System services available to BASE I and to SMS users. Service descriptions include basic information, processing requirements, options, features, key message fields, and message flows. Volume 2 contains the following parts: Part 6: Authorization Database Files and Services Part 7: Authorization Services Doc ID 0853B-04

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

BASE I
V.I.P. System BASE I Processing Specifications Describes V.I.P. transaction processing in the BASE I System environment, including message types, processing considerations, security responsibilities, related services, and connection options. Doc ID 0847-04
V.I.P. System BASE I Technical Specifications, Volume 1 Documents technical specifications of V.I.P. transaction processing in the BASE I System environment. This companion volume to *V.I.P. System BASE I Processing Specifications* describes the fields for BASE I. Doc ID 0844A-05
V.I.P. System BASE I Technical Specifications, Volume 2 Documents technical specifications of V.I.P. transaction processing in the BASE I System environment. This companion volume to *V.I.P. System BASE I Processing Specifications* describes the message formats and file specifications for BASE I. Doc ID 0844B-05
Interlink
V.I.P. System SMS Processing Specifications (U.S.) Contains information about the Single Message System, including message types, processing considerations, connection options, security responsibilities, and related services for Visa/Plus ATM, Interlink, Visa POS, and Visa Electron. Doc ID 0857-04
V.I.P. System SMS Interlink Technical Specifications Companion volume to *V.I.P. System SMS Processing Specifications (U.S.)*. Describes message formats, field descriptions, and file specifications for Interlink. Doc ID 0866-03
SMS ATM
V.I.P. System SMS Processing Specifications (U.S.) Contains information about the Single Message System, including message types, processing considerations, connection options, security responsibilities, and related services for Visa/Plus ATM, Interlink, Visa POS, and Visa Electron. Doc ID 0857-04

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

V.I.P. System International 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 0839-04

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

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

Doc ID 0868A-03

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

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

Doc ID 0868B-03

SMS POS

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

Contains information about the Single Message System, including message types, processing considerations, connection options, security responsibilities, and related services for Visa/Plus ATM, Interlink, Visa POS, and Visa Electron.

Doc ID 0857-04

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

Contains information about Single Message System POS processing, including message types, processing considerations, connection options, security responsibilities, related services, and reports.

Doc ID 0835-04

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

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

Doc ID 0869A-03

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

V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 2
Companion volume to *V.I.P. System SMS Processing Specifications (U.S.)* and to *V.I.P. System International SMS POS (Visa & Visa Electron) Processing Specifications*. Describes message formats and file specifications for Visa POS and for Visa Electron.
Doc ID 0869B-03

SOURCES OF V.I.P. INFORMATION

This section lists the primary sources for the information contained in the *V.I.P. System Overview*. 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 revised manual incorporates all of the comments and change requests received from members and from Visa staff, where appropriate.

Existing Manuals

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

Technical Letters

The *V.I.P. System Overview* includes information from the following technical letters:

- *October 2003 VisaNet Business Enhancements Technical Letter*, publication 80019-02, including Update Bulletins
- *April 2004 VisaNet Business Enhancements Technical Letter*, publication 80022-02, including Update Bulletins

Other Documents

Other documents used as sources for the *V.I.P. System Overview* include:

Address Verification Service Business Context

Address Verification Service User's Guide

CPS/ATM for BASE I and BASE II Members Member Implementation Guide

Payment Technology Standards Manual

POS Check Service Planning Guide

The Road to Chip: An Employee Guide to Visa Smart Card Development

Visa Horizon Brochure and Fact Sheets

Visa Operating Regulations (and all revisions)

Other sources include RTN publications, general design documents, detailed design documents, service advisories, and project presentations.

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

- U.S. members and third-party processors can contact the Visa U.S.A. Member Publications department by sending an e-mail to puborder@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@visa.com. Docline distributes VisaNet documentation and tries to locate other publications distributed elsewhere within Visa.
- Visa staff located in Miami and outside of the U.S. can contact their regional representatives.

To inquire about VisaNet documentation or to submit changes and additions, contact Technical Communications Services by sending an e-mail to Docline@visa.com.

Operating Regulations

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

Visa International Operating Regulations

The *Visa International Operating Regulations* consists of four volumes of operating regulations covering all Visa regions *except* the U.S. region, namely:

- Volume I—General Rules
- Volume II—Dispute Resolution Rules
- Volume IV—Interlink Program Operating Regulations
- Volume V—Visa Cash Program Operating Regulations

Regions are also governed by the regulations in *Visa International Card and Marks Specifications*.

For More Information

The *Visa Regional Operating Regulations* refers to operating regulations for each of the Visa regions *except* the U.S. region, namely:

- Visa Regional Operating Regulations—Asia-Pacific (AP)
- Visa Regional Operating Regulations—Canada (CAN)
- Visa Regional Operating Regulations—Central and Eastern Europe, Middle East, and Africa (CEMEA)
- Visa Regional Operating Regulations—European Union (EU)
- Visa Regional Operating Regulations—Latin America and Caribbean (LAC)

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

The *Visa U.S.A. Inc. Operating Regulations* consists of two volumes of operating regulations for the U.S. region *only*:

- Volume I—General Rules
- Volume II—Dispute Resolution Rules

The U.S. region is also governed by the *Visa U.S.A. Inc. By-Laws*.

BackOffice Adjustment System (BOAS)—DOS Version

For information about BOAS, refer to:

BOAS Administration and Technical Guide

Using BOAS With the BASE II System

Using BOAS With the Single Message System

BackOffice Adjustment System (BOAS) OnLine

For information about BOAS OnLine, refer to:

BOAS OnLine Conversion Guide—Legacy Members

BOAS OnLine Member System Administrator's Guide

BOAS OnLine User's Guide

Deferred Clearing Advice File (DCAF) Service

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

POS Check Service

For information about the POS Check Service, refer to:

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

V.I.P. System Services, Volume 2

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

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

For More Information

Risk Management Services

For information about risk management services, refer to:

Card Recovery Bulletin Service User's Guide

Fraud Reporting System User's Manual

Issuer's Clearinghouse Service User's Guide

National Merchant Alert Service User's Guide

Risk Identification Service User's Manual

Risk Management Process Guide

V.I.P. System Services, Volume 1

Visa Issuer Fraud Detection (VIFD) Service Workstation User's Guide

Security

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

Introduction to Cryptography and PIN Security

Payment Technology Standards Manual

PIN Security Program: Auditor's Guide

PIN Security Requirements

Visa Image Exchange Workstation (VIEW)

For information about VIEW and about VIEW OnLine, refer to:

Visa Image Exchange Workstation (VIEW) Administrator's Guide

Visa Image Exchange Workstation (VIEW) Installation Guide

Visa Image Exchange Workstation (VIEW) User's Guide

Visa Image Exchange Workstation (VIEW) OnLine Thick Client User's Guide

Visa Image Exchange Workstation (VIEW) OnLine Thick Client Member Implementation Guide

Visa Image Exchange Workstation (VIEW) OnLine Thin Client User's Guide

Visa Image Exchange Workstation (VIEW) OnLine Thin Client Member Implementation Guide

Visa Smart Debit/Smart Credit (VSDC) Service

For information about the VSDC Service, refer to:

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

For More Information

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

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

Visa Smart Debit and Credit Member Implementation Guide for 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.

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

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

VisaNet Access Points (VAPs)

For information about VisaNet Access Points (VAPs), refer to the pertinent sets of documentation listed below. 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 and Other File Processing

VAP Interface Specifications: V.I.P. Processing

VAP Messages and Troubleshooting

VAP Operator's Guide

VAP Software Library

VAP Systems Guide

VAP Release 11 Documentation

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

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

VAP Release 11 Maintenance, Messages, and Troubleshooting Guide

VAP Release 11 Operator's Guide

For More Information

VisaNet Copy Request and Fulfillment Service (VCRFS)

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

VCRFS Fax Gateway User's Guide

VCRFS Processing Guide

VisaNet Image Gateway Image Interface Technical Specifications

VisaNet Image Gateway User's Guide

Miscellaneous Systems and Services

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

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

Visa Global ATM Planning 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.

Address Verification Service (AVS) User's Guide

Card Verification Value (CVV) Member Technical Guide

Cardholder Verification Value Reporting User's Guide

Cash-Back Service Description (Doc ID 40080-01)

Visa Information System User's Guide

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

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

Visa Test System - Version 3 User's Guide

VTS2000 User's Guide

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 1

V.I.P. System Basics

This chapter provides a description of VisaNet, transaction process flows, and Visa products. It also describes VisaNet components and VisaNet processing systems.

1.1 VISANET OVERVIEW

VisaNet is the Visa transaction processing network. The term applies to all components of the network, from the hardware, software, and communications facilities that connect the Visa network with members' systems and with other networks, to the systems that perform all transaction processing and system services. VisaNet routes transactions between acquirers and issuers through its global transaction processing network.

VisaNet supports:

- Purchase and cash transactions made with any Visa card.
- Purchase transactions made with major travel and entertainment (T&E) cards.
- ATM transactions for other networks (such as Plus).
- Purchase and cash transactions made with other private-label and proprietary cards.

These transactions are processed through VisaNet's authorization, clearing, and settlement services, which are available to members in all Visa regions. Visa defines these basic services as follows:

- *Authorization* is when the issuer approves or declines a sales transaction before a purchase is finalized or cash is disbursed.
- *Clearing* is when a transaction is delivered from an acquirer to an issuer for posting to the cardholder's account.
- *Settlement* is the process of calculating and determining the net financial position of each member for all transactions that are cleared. The actual exchange of funds is a separate process.

Transactions can be authorized, cleared, and settled as either dual-message or single-message transactions.

- A *dual-message transaction* is sent twice, the first time with only the information needed for an authorization decision, and again later with additional information required for clearing and settlement. Typically, authorization is performed online while clearing and settlement occur later offline.
- A *single-message transaction* is sent once for authorization and contains clearing and settlement information as well as authorization information. These transactions are also called "full financial" transactions. Typically, authorization and clearing occur online, while settlement occurs later offline.

  Single-message transactions may also be processed using online *deferred clearing*. In this case, transactions are authorized online and cleared and settled at a later time.

  Deferred clearing can be used for transactions for which the final purchase amount is not known at the time of authorization; for instance, for transactions submitted by hotels and by car rental agencies.

NOTE

Only Visa point-of-sale or point-of-service (POS) and Visa Electron acquirers can submit deferred clearing transactions. However, an issuer can receive deferred clearing advices for ATM transactions if they do not participate in the ATM Format Conversion Service. Refer to the ATM Format Conversion Service chapter in V.I.P. System Services, Volume 2, *for information about this service.*

For more information about POS and Visa Electron transactions, refer to V.I.P. System SMS Processing Specifications (U.S.) *or to* V.I.P. System International SMS POS (Visa & Visa Electron) Processing Specifications.

1.2 VISA PRODUCTS

This section briefly describes the various Visa products that are referenced in this book. Visa also offers many other products that are not described here as well as product platforms such as chip cards.

Visa offers products that access a cardholder's line of credit as well as a cardholder's checking or savings account. Visa products include:

Visa Cash—Visa Cash is a global chip-based electronic purse card program that can be used for small-ticket payments and cash access at the POS or at an ATM. The service uses a smart card to store monetary value. The amount of each purchase is automatically deducted from the cardholder's balance. Purchases do not require a signature or a PIN.

Visa Debit—Visa Debit (known in the United States [U.S.] region as Visa check card II) is a debit card program accepted at any Visa merchant or ATM location. The amount of each purchase is automatically deducted from the cardholder's deposit account. POS purchases require a signature or a PIN, and ATM cash disbursements require a PIN.

Visa Electron—Visa Electron is a global acceptance mark that can be used for payment and for cash access in electronic merchant environments and through the Visa Global ATM Network. All transactions are authorized by the issuer and are verified by the cardholder with either a PIN or a signature.

Visa Horizon—Visa Horizon is a single currency payment application that can be used both for cash disbursements and for purchases. The service uses chip cards and VSDC-capable terminals and ATMs. Issuers determine cardholder spending limits, and all transactions require a PIN.

Visa Interlink—Visa Interlink (known in the U.S. region as Interlink) is a single-message deposit access service that offers all electronic processing at the POS. Cardholders can use their ATM card to make purchases at participating retail locations and to request cash back from their purchase. Interlink requires the cardholder to enter a PIN.

Plus—Plus is an ATM card program available to Visa members worldwide. Plus System, Inc., using the Plus network, provides ATM interchange for cards bearing the Plus logo. Plus access requires PIN verification.

Table 1-1 compares the Visa products referenced in this book.

Table 1-1 Comparison of Visa Products

Visa Product	Type of Processing	Cardholder Identification	Acceptance Environment
Visa Cash	Dual- or single-message	• None for POS transactions • PIN for ATM transactions	• ATM • POS
Visa Debit **(Visa check card II)**	Dual- or single-message	• Usually signature for POS transactions, but PIN can be accepted • PIN for ATM transactions	• ATM • POS
Visa Electron	Dual- or single-message	• Usually signature for POS transactions, but PIN can be accepted • PIN for ATM transactions	• ATM • POS
Visa Horizon	Dual-message	• PIN for POS transactions • PIN for ATM transactions	• ATM • POS
Visa Interlink	Single-message	PIN	POS
Plus	Dual- or single-message	PIN	ATM

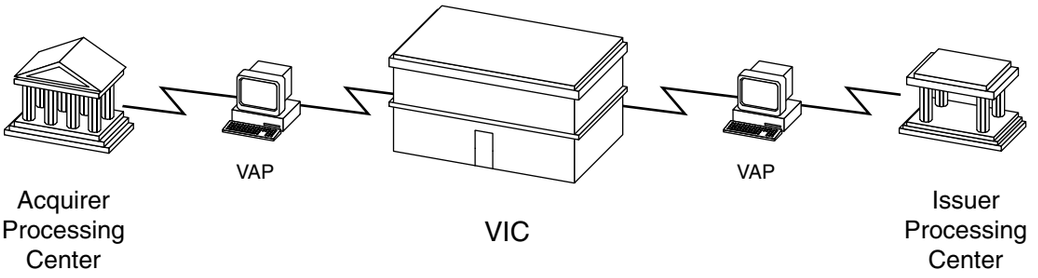
1.3 VISANET COMPONENTS

The main components of VisaNet are:

- VisaNet Interchange Centers (VICs).
- VisaNet Access Points (VAPs) and other network connections.
- Processing centers.

Figure 1-1 illustrates the VisaNet communications network.

Figure 1-1 The VisaNet Communications Network



VisaNet Interchange Centers (VICs)—A *VIC* is a Visa data processing center. There are four VICs: two in the United States, one in the United Kingdom, and one in Japan. Each VIC houses the computer systems that perform all VisaNet transaction processing. The VIC serves as the control point for the telecommunications facilities of the VisaNet Communications Network, which comprises high-speed leased lines or satellite connections based on IBM SNA and TCP/IP protocols.

VisaNet Access Point (VAP)—A *VAP* is a Visa-supplied small computer system (located at the processing center) that provides the interface between the center's host computer and the VIC. The VAP facilitates the transmission of messages and files between the center host and the VIC, supporting the authorization, clearing, and settlement of transactions. Visa also provides other connection options for interacting with VisaNet that do not require VAPs. Options vary by region. Members can contact their Visa representatives for available options.

For information about VAPs, refer to About This Manual for a list of VAP documents.

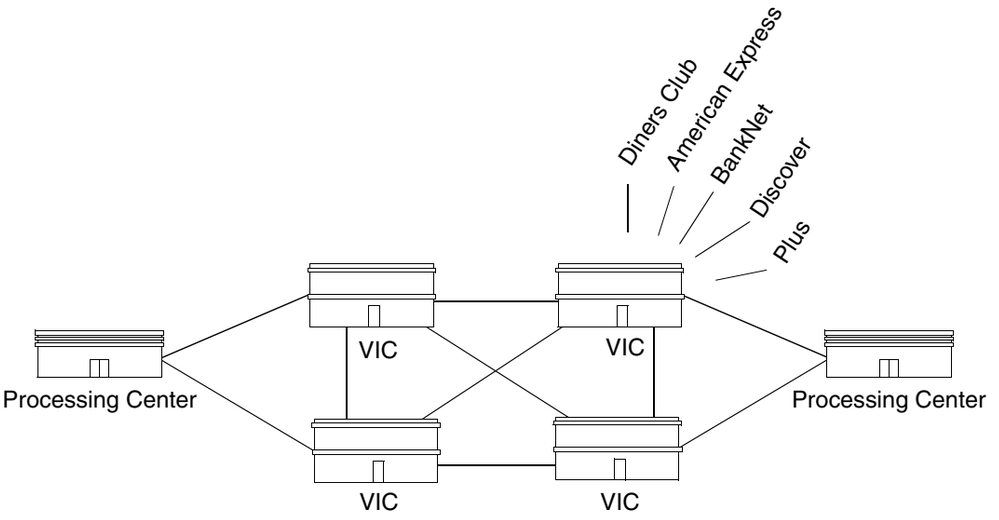
Processing Center—A *processing center*, also referred to as simply a center, is a data processing facility operated by or designated by an issuer or an acquirer. The processing center houses card processing systems that support merchant and business locations and maintain cardholder data and billing systems.

Each processing center communicating with VisaNet is linked to two VICs. Centers are connected to the closest, or primary, VIC. If one VIC experiences system interruptions, VisaNet automatically routes members' transactions to a secondary VIC, ensuring continuity of service.

Each VIC is also linked to all of the other VICs. This link enables processing centers to communicate with each other through one or more VICs. Processing centers can also access the networks of other card programs through the VIC.

Figure 1-2 illustrates how communication flows between the processing centers and the VICs.

Figure 1-2 VisaNet Communication Flows



VisaNet operates 24 hours a day throughout the year. Visa provides the following backup capabilities:

- Visa backs up VAP systems.
- Visa backs up the V.I.P. lines from the VAPs to the VICs.
- VICs back up each other.

In addition, the VisaNet network ensures that all of its links have multiple backups. The connection from one point in the network to another is not usually a fixed link; instead, VisaNet chooses the best possible path at the time of any given transmission. Rerouting around any failed line occurs automatically.

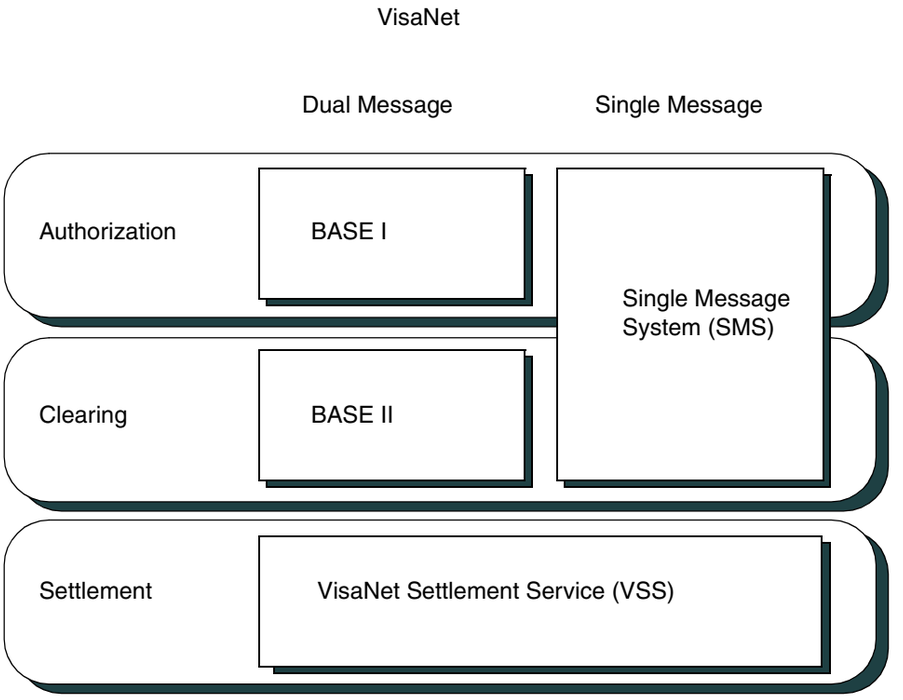
1.4 VISANET SYSTEMS

The VICs house the following VisaNet systems that provide both online and offline transaction processing:

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

These VisaNet systems perform authorization, clearing, and settlement, as shown in Figure 1-3.

Figure 1-3 VisaNet Systems and Transaction Processing



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

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

V.I.P. has one system that supports *single-message processing* (the processing of interchange card transactions that contain both authorization and clearing information in a single message), and another system that supports *dual-message processing* (authorization of transactions is requested in a first message, while financial clearing information is sent in a second message). In both cases, settlement occurs separately.

1.4.1.1 BASE I System

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

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

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

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

NOTE

BASE I is not used for Interlink transaction processing.

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

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

BASE I Offline Functions—The BASE I offline functions include BASE I reporting and generating Visa Card Recovery Bulletins. BASE I reporting includes authorization reports, Exception File and Advice File reports, and POS reports. For more information about BASE I offline functions, refer to *V.I.P. System BASE I Processing Specifications* and to *V.I.P. System BASE I Technical Specifications*.

1.4.1.2 Single Message System (SMS)

The Single Message System (SMS) component of the V.I.P. System processes full financial transactions. *Full financial* transactions contain both authorization and clearing information. Because the authorization and clearing information is contained in one message, this form of processing is referred to as *single-message processing*. SMS (formerly called Debit) also supports dual-message processing of authorization and clearing messages, communicating with BASE I and accessing outside networks, as required, to complete transaction processing. *Only* the SMS component performs single-message processing.

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

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

SMS supports online functions, offline functions, and the SMS files. The SMS files comprise internal system tables that control system access and processing, and the SMS Cardholder Database, which contains files of cardholder data used for PIN verification and for stand-in processing (STIP) authorization.

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

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

SMS Offline Functions—The SMS offline systems process settlement and funds transfer requests and provide settlement and activity reporting. They also support an offline bridge to and from BASE II for those Visa and Plus clearing transactions that are sent between an SMS member and a BASE II member.

Both the BASE I and the SMS components use files of member-supplied cardholder data and processing parameters to perform online processing. Both systems interact with 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 "*More Information*" section of* About This Manual *for a list of BOAS documents.*

SMS processes Visa, Plus, Interlink, and other card transactions.

NOTE

SMS endpoints must use the V.I.P. ISO (International Organisation for Standardisation) message format and must observe all rules for its use.

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

1.4.2 BASE II System

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

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

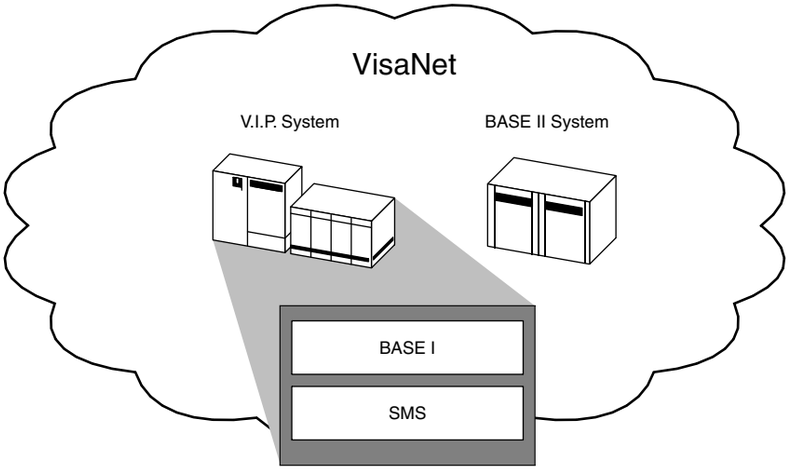
NOTE

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

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

Figure 1-4 illustrates how V.I.P. and its software system components, along with BASE II, reside in the VisaNet network.

Figure 1-4 The VisaNet Software System Components



Visa members and processors that use BASE I and BASE II may choose to use SMS to process some of their transactions, or to use different processing methods for different Visa products.

EXAMPLE

An issuer can use BASE I and BASE II processing for credit products, and use SMS processing for debit products.

1.4.3 VisaNet Distributed Processing System (VDPS)

The VisaNet Distributed Processing System (VDPS) is a scalable, distributed, regionally-based alternative to the V.I.P. System that provides dual-message and single-message online processing. VDPS is part of VisaNet. Regions and countries within regions can choose whether to use VDPS or to use the V.I.P. System for intra-regional or for domestic online processing.

VDPS is functionally similar to V.I.P. and supports a robust suite of online processing options, including:

- Visa, Visa Electron, and Plus production support
- Stand-in processing
- Authorization services, such as Address Verification Service, Card Verification Value Service, and PIN Verification Service
- Multicurrency Service
- Gateway Services

Cardholder transactions are sent between VDPS and V.I.P. depending on destination. VDPS forwards to V.I.P. messages destined for V.I.P.-connected participants, and V.I.P. forwards to VDPS messages destined for VDPS-connected participants.

Members can contact their Visa representatives for more information about VDPS.

VDPS acquirers and issuers connect to VDPS just as members connect now to V.I.P. The following subsection introduces various V.I.P. and VDPS access methods.

1.4.4 The Common Member Interface (CMI) and Other Access Methods

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

The CMI processes BASE I messages *and* SMS messages. CMI processing in V.I.P. routes messages to their BASE I or SMS destinations, depending on the type of processing requested, and to the processing network in cases when the message specifies a network other than VisaNet (for instance, the MasterCard Banknet network).

NOTE

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

The CMI accepts messages in BASE I-specific format, SMS-specific format, and V.I.P format (the message format common both to BASE I and to SMS). Functions of CMI include basic editing as well as routing.

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

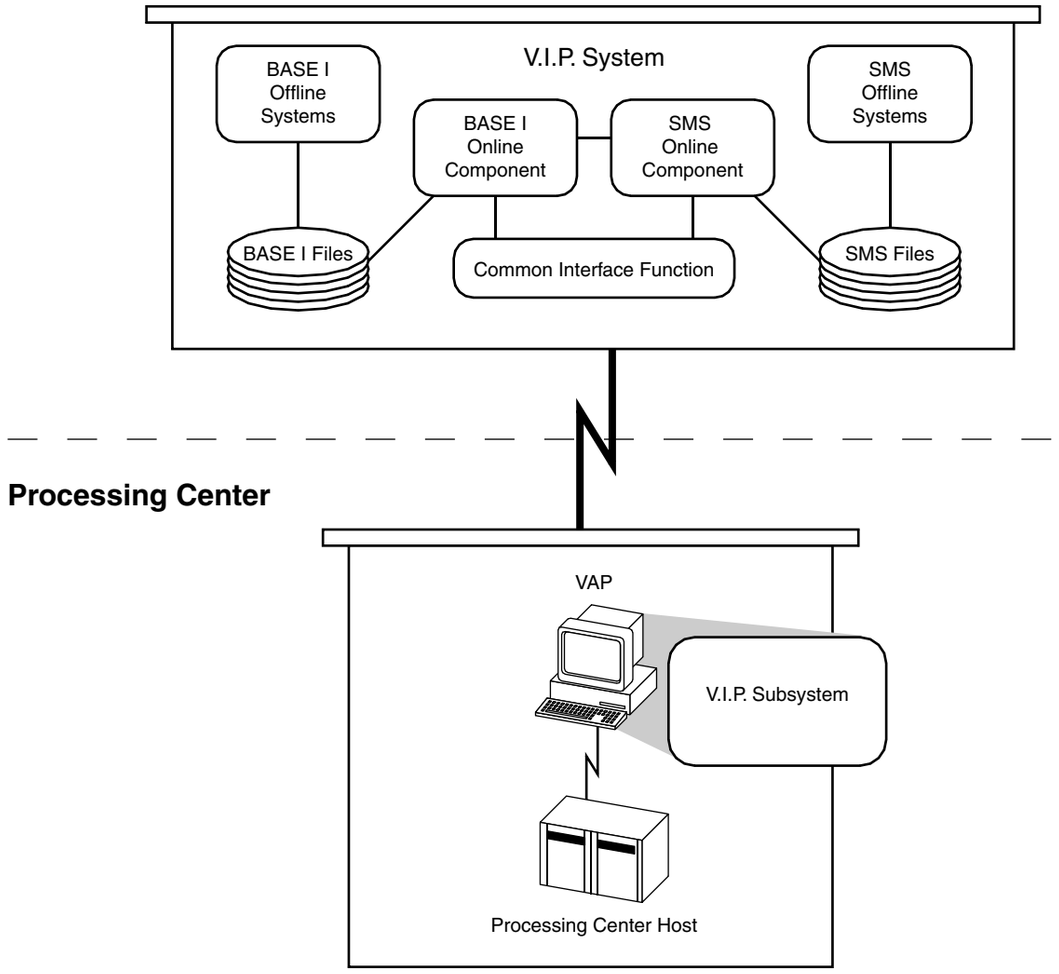
Besides the CMI, other access methods available to members and to processing centers are:

- BASE I only.
- SMS only.

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

Figure 1-5 illustrates the V.I.P. system software components. In the example, the processing center uses a single system both for BASE I and for SMS processing.

Figure 1-5 VIP System Software at the VIC and at the Processing Center



1.4.5 VisaNet Settlement Service (VSS)

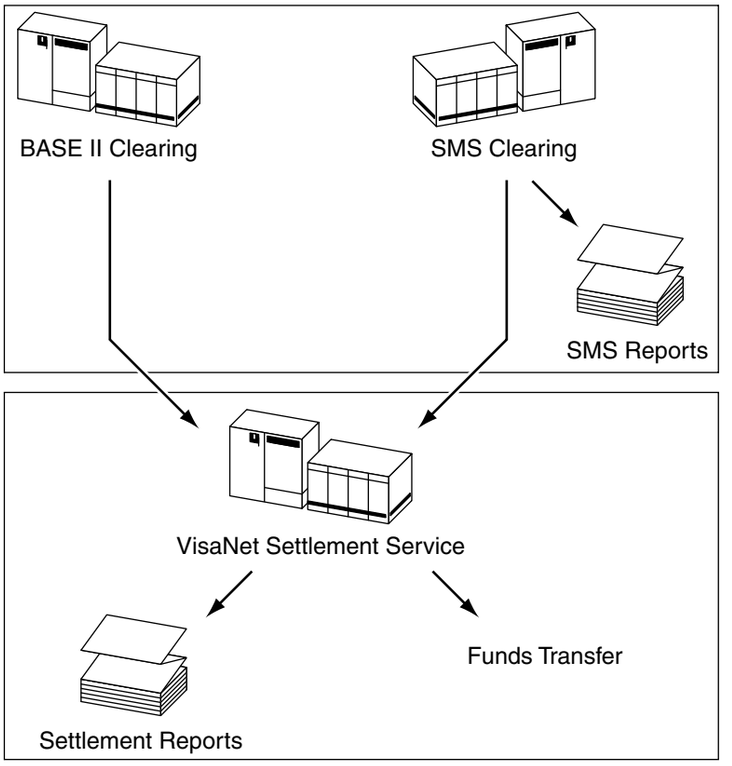
The VisaNet Settlement Service (VSS) consolidates the settlement functions of SMS and of BASE II, including Interlink, into a single service for all products and services. Members and processors receive settlement information from SMS and from BASE II in a standardized set of reports. VSS provides flexibility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

Visa processes interchange transactions for SMS and for BASE II through separate systems. Both SMS and BASE II perform their own clearing functions. 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. Clearing also includes *valuation*, the calculation of many types of fees and charges.
- *Settlement* is the process of calculating and determining the net financial position of each member for all transactions that are cleared.

Figure 1-6 illustrates the VSS clearing and settlement process.

Figure 1-6 VisaNet Settlement Service (VSS) Process



1.4.6 V.I.P. Processing Parameters

Members and system users control both BASE I and SMS processing primarily by selecting options and by establishing limits and parameters. V.I.P. executes the majority of system functions according to parameters selected by the users. Most V.I.P. services offer users many options for implementing and for operating the service.

Some services allow users to choose different options by BIN (that is, by a specific range of card numbers for a specific card program). Other options apply to all messages processed by a given processing center. Additional options enable individual stations at processing centers to handle specific types of transactions.

V.I.P. maintains records of routing and processing rules that apply to BINs, to processing centers, and to stations. These parameters are stored in the *system tables* (often called the system globals or system files). Typically, multiple BINs point to a single processing center. Users change their parameters as needed to reflect business changes.

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

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

Users report any changes in account number ranges or in processing center designations to Visa. This information is vital to the correct routing of messages.

1.4.7 V.I.P. Messages

Information passes between members and V.I.P. in the form of BASE I and SMS messages. Both BASE I and SMS messages are Visa variations of the International Organisation for Standardisation (ISO) 8583 message, the international standard for the format of financial messages. Each message contains bit maps that specify the data fields that appear in the message, a message type identifier, and only those fields that are needed for the specific function intended.

V.I.P. checks each message for validity and edits messages as required. The CMI performs message format conversion, if necessary.

Maintaining message integrity is critical to V.I.P. processing. Message integrity assures participants that all other participants have followed Visa processing rules and that a participant can act on a message or a transaction as defined.

All participants keep track of incoming and outgoing messages.

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 2

V.I.P. Transaction Processing

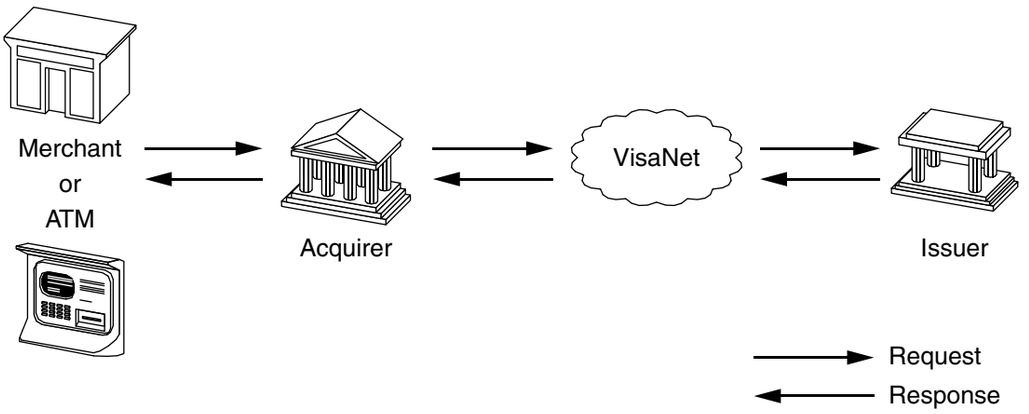
This chapter describes transaction flows, V.I.P. message format and structure, and V.I.P. message processing including stand-in processing (STIP) and routing. It also describes additional V.I.P. functions such as managing system tables and system databases, and reporting.

2.1 TRANSACTION FLOW

This section describes the transaction flow between an acquirer and an issuer for a purchase at a merchant location. This discussion is a high-level explanation; transaction processing steps vary depending on the complexity of the transaction and on the processing services used.

Figure 2-1 illustrates a typical transaction processing flow.

Figure 2-1 VisaNet Basic Process Flow



1. The transaction begins when a card is inserted at an ATM or is swiped or keyed at a point-of-sale or point-of-service (POS) terminal. The terminal prompts the cardholder for a personal identification number (PIN), if applicable.
2. The merchant creates a financial request message and forwards it to the acquirer. The request includes the transaction type, the merchant name, the encrypted PIN, and the transaction amount.
3. The acquirer logs the request, excluding the PIN information, and forwards the message to VisaNet.
4. The V.I.P. System logs the transaction, performs currency conversion if requested, and routes the message to the issuer. Routing is based on the card number and on selected routing options for the acquirer and for the issuer. V.I.P. may route the transaction to STIP instead of to the issuer for processing, depending on issuer and Visa options for processing in issuer-available and issuer-unavailable conditions.
5. The issuer verifies the PIN, checks the transaction amount against the account's available balance or open-to-buy balance, and checks daily activity limits and other controls, if any. The issuer logs the transaction and, for approved transactions, places a hold on the funds or reduces the cardholder's available balance by the amount of the transaction. The issuer creates an authorization or a financial response message based on the results of these edits and sends it to VisaNet.
6. V.I.P. logs the message and forwards it to the acquirer.
7. The acquirer logs the financial response and forwards it to the merchant to complete the transaction. The acquirer ensures that the response is successfully delivered. If the cardholder did not enter a PIN earlier, the cardholder's signature is required.

2.2 V.I.P. MESSAGE PROCESSING

When V.I.P. receives a message, it performs the following main functions:

- Message validation and preparation
- Message routing
- Stand-in processing (STIP), as required
- Response processing and logging

The following subsections describe these functions.

2.3 MESSAGE VALIDATION AND PREPARATION

V.I.P. checks the format and the content of each message it receives. Every message must comply with the V.I.P. System message requirements for the message type. Also, each processing station must use either BASE I or V.I.P. format specifications and all messages from that station must comply with the requirements for that format's specifications.

If the message format is incorrect, V.I.P. returns it to the sender with the appropriate reject code indicating why the message was rejected. If the message format is correct, V.I.P. performs additional edits and prepares the message further. For instance, for Single Message System (SMS) financial messages, V.I.P. inserts a settlement date.

V.I.P. also performs member- or Visa-designated functions such as:

- Message enhancement
- Chip authentication
- PIN verification
- PIN translation
- Card Verification Value (CVV), Card Verification Value 2 (CVV2), and Integrated Circuit Card CVV (iCVV) verification
- Cardholder Authentication Verification Value (CAVV) verification
- Currency conversion
- Reimbursement program screening

Once a message is validated, it is ready to be routed.

Refer to *V.I.P. System Services* for complete service information for Card Verification Value (CVV) Service, Card Verification Value 2 (CVV2) Service, PIN verification methods, PIN Verification Service (PVS), Multicurrency Service, and Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure).

2.3.1 Message Formats

Issuers and acquirers format messages according to Visa standards. V.I.P. System message formats and content are based on International Organisation for Standardisation (ISO) 8583 requirements. V.I.P. supports two message formats:

BASE I Message Format—This message format is only supported by BASE I.

V.I.P. Message Format—This format is supported both by BASE I and by SMS. This format enables members to use both processing systems for their transactions depending on their preferences. The V.I.P. message format provides enhanced processing capabilities to members and to processors.

IMPORTANT

All centers, BASE I or SMS, that are connecting to the V.I.P. System for the first time are required to use the V.I.P. message format.

Refer to *V.I.P. System BASE I Technical Specifications* and to the V.I.P. System SMS technical specifications manuals for details about message formats.

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

2.3.2 V.I.P. Message Structure

Messages are bit-mapped so they transmit only appropriate data. Table 2-1illustrates the message elements that each bit-mapped message contains.

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

Message Header	Message Type Identifier	Bit Maps	Data Fields

Message Header—The message header contains basic message identifiers and routing information along with message processing control codes and flags.

Message Type Identifier—The message type identifier specifies the message class and category of function. For instance, 0100 indicates an authorization request. All messages contain a message type identifier.

Bit Maps (one or more)—A bit map specifies which data fields are in a message. In addition to a primary bit map, messages can include second and third bit maps. Each map contains 64-bit fields, corresponding to the number of possible fields in a message.

Data Fields—The data fields contain the information needed to process a message.

Differences between BASE I and V.I.P. message formats and their individual field requirements are detailed in *V.I.P. System BASE I Technical Specifications* and in the V.I.P. System SMS technical specifications manuals.

2.3.3 Message Matching

V.I.P. System transactions generally consist of pairs of messages: a request message followed by a response message. The V.I.P. System compares information in key data fields to match messages within a transaction.

Message sets provide the acquirer, the issuer, and V.I.P. with the means to link messages and to control real-time account posting and settlement accumulator updating. For a cardholder transaction, processors must use only the messages allowed in the associated transaction set. V.I.P. uses message matching to prevent invalid messages within a transaction and to ensure transaction integrity.

2.4 MESSAGE ROUTING BASICS

Message routing is an important function of the V.I.P. System. *Routing* refers to sending messages between VisaNet and acquirer and issuer processing centers. Routing also refers to sending a message to V.I.P. stand-in processing (STIP) for authorizing a transaction on an issuer's behalf.

2.4.1 Routing Messages

To route messages, V.I.P. uses member-supplied information stored in the BASE I and SMS system tables along with information in the message header, the message type identifier, and data fields. V.I.P. compares the message information to the applicable BIN (a range of card numbers for a specific card program, such as Visa Classic) and to processing center information stored in the system tables. This information includes:

- Account number.
- Card type.
- Source address.
- Destination address.

Visa assumes responsibility for routing a request to its proper destination. Acquirers do not have to determine the destination of their authorization or financial requests because V.I.P. routes requests based on the account number in the message.

NOTE

In some cases, V.I.P. uses data other than the account number to determine message routing.

EXAMPLE

For SMS transactions, V.I.P. also uses the value in the network ID field to route messages.

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

2.4.1.1 System Tables Routing Information

To route messages, both BASE I and SMS access member information stored in the BASE I and the SMS system tables. These tables contain records of the relationships of issuers to account numbers, of issuers and acquirers to processing centers, of processing centers to the VICs, and of processing centers to stations.

2.4.1.2 Routing Tables

V.I.P. provides routing table services for acquirers. The *routing tables*, also referred to as BIN tables or as account range tables, are batch data files that list all card prefixes, prefix lengths, and account number lengths. The tables help V.I.P. and acquirers make authorization routing decisions.

The current routing tables are:

- Visa
- Plus BIN Table
- Combined Visa/Plus
- Visa Electron
- Interlink
- Visa POS Debit Device

Members control VisaNet processing by the parameters and the options (which are stored in the tables) they select. Members also control routing by establishing appropriate relationships among card account number ranges, types of transactions, and processing center stations. Factors used by BASE I and by SMS for routing Visa, Visa Electron, Plus, and Interlink transactions, as well as those for non-Visa card products, include:

- Routing and transit numbers.
- Network IDs.
- Card types.
- Account ranges.
- Processing centers.
- Acquirer and issuer stations.
- User preferences for priority routing and for PIN processing.

Acquirers use routing tables to determine which transactions should be sent to VisaNet for processing. Entries in the Visa and Plus BIN routing tables consist of whatever number of digits that are required to identify a card range or a card portfolio. A routing table entry may be

simply a BIN (for instance, 412345), or may be a longer number for a Plus proprietary card program (for instance, 504667214). Entries can be up to 12 digits.

Visa and Plus acquirers are required to use the Visa and Plus routing tables. Visa POS acquirers in the U.S. region are required to use the Visa POS Debit Device routing table. For more information about routing tables, refer to the *Visa Operating Regulations*. Members can contact their Visa representatives to obtain the tables.

2.4.1.3 Internal Routing Services

In addition to basic routing functionality, Visa provides a variety of routing services that enable issuers and acquirers to specify alternate routing for transactions with specified characteristics. Most of the routing services V.I.P. provides are optional.

EXAMPLE

Issuers can designate an alternate path for routing particular transaction types. For instance, ATM transactions can be routed differently from POS transactions; PIN transactions can be routed differently from non-PIN transactions; exception transactions can be routed differently from authorizations and financial transactions.

Additionally, V.I.P. can route transactions according to member specifications using either the Positive Cardholder Authorization Service (PCAS) or the Positive Authorization Capacity Management (PACM) Service. These services route low-risk transactions to the V.I.P. stand-in processor (STIP):

- PCAS routes transactions to the issuer or to STIP using issuer limit dollar amounts.
- PACM routes transactions to the issuer or to STIP primarily using a dynamic limit called the *Diversion Threshold*. STIP determines this limit by comparing transaction volume to issuer capacity.

Refer to *V.I.P. System Services, Volume 1 and Volume 2*, for an overview of routing services and for complete descriptions about all routing services. Refer also to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals for additional information about V.I.P. routing.

2.4.1.4 Gateways to Non-VisaNet Destinations

If the destination is a system or a network outside of VisaNet, V.I.P. uses Gateway Services to reformat the message, if necessary, and to deliver it to the other system or network. Both BASE I and SMS have connections, or *gateways*, to outside systems and networks. Gateway Services route transactions through these gateways and return messages to members using the same VisaNet connection point.

Refer to Part 2 of *V.I.P. System Services, Volume 1*, for detailed information about available gateways and Gateway Services.

2.5 STAND-IN PROCESSING (STIP)

V.I.P. acts as a backup processor when requested by issuers or when issuers are unavailable. During this backup processing, V.I.P. authorizes, declines, or refers transactions on the issuer's behalf. This function is referred to as *stand-in processing*, or *STIP*.

Issuers specify the stand-in processing parameters that V.I.P. is to use. Visa card issuers can maintain files of cardholder data at the VisaNet Interchange Center (VIC) and can select the

limits that control which transactions can be approved in STIP. Other card programs processed according to Visa rules are also eligible for STIP at the issuer's discretion.

Whether a transaction is routed to the issuer or to STIP for an approval or a decline decision depends on the:

- Availability of the issuer at the time the transaction is being processed.
- Issuer-specified transaction processing parameters that reside in the system tables.
- Visa-mandated conditions for certain transaction types.

If the conditions of the cardholder account and the transaction require that the issuer, rather than STIP, should make the final authorization decision, STIP forwards the request message to the issuer if the center is available. If the issuer is unavailable, STIP then processes the transaction according to issuer-unavailable parameters.

V.I.P. usually creates advices for issuers to inform them of actions taken by STIP on their behalf. Issuers may recover their advice data from V.I.P. Refer to *V.I.P. System Services, Volume 2*, for information on both BASE I and SMS advice retrieval services.

Visa provides issuers with two, optional, issuer-or-STIP routing services that can assist in the routing decision process:

- Positive Authorization Capacity Management (PACM) Service—This BASE I and SMS service routes authorization and financial requests based on dollar amount thresholds and on message traffic volumes.
- Positive Cardholder Authorization Service (PCAS)—This BASE I service routes authorization requests to the issuer or to STIP according to a comprehensive set of risk control parameters that includes dollar amount thresholds.

Refer to *V.I.P. System Services, Volume 2*, for information about these services.

2.5.1 BASE I STIP

BASE I stand-in processing (STIP) provides issuers with business functions that:

- Protect issuers from transaction volumes in excess of their processing capacity.
- Allow issuers to control authorization processing expenses by having STIP approve low-risk, small-ticket transactions.
- Allow issuers to provide a high level of cardholder service during issuer-unavailable conditions while still controlling risk.

The first two functions pertain largely to *issuer-available* STIP. The third function applies largely to *issuer-unavailable* STIP. The different circumstances and implications between issuer-available and issuer-unavailable processing drive the rules for how transactions are processed.

When transactions fail issuer-available STIP processing, V.I.P. typically (at the issuers' option) forward-refers them to issuers for authorization decisions. In these cases, STIP forward-refers transactions identified as having elevated risk to the issuer and approves transactions within issuer-unavailable risk parameters. This approach minimizes negative cardholder experiences resulting from false declines; that is, declining a "good" cardholder because of transaction characteristics or because of cardholder spending that indicates heightened risk.

When the issuer is unavailable, STIP cannot forward-refer transactions to the issuer. Instead, it must generate a response for the acquirer. This circumstance creates an elevated customer

service risk. Thus, for issuer-unavailable processing, issuers may choose to relax cardholder spending-related risk controls for the sake of increasing customer service levels.

BASE I STIP performs a number of functional services to identify elevated risk. These services include:

- Checking the CVV or the iCVV, CAVV, PIN, expiration date, and BASE I Exception File.
- Validating the account number with the Luhn modulus-10 algorithm.
- Checking cardholder spending and activity, and the transaction amount.

BASE I STIP provides a wide variety of issuer options for determining which of these functions are performed and how they are used.

Refer to *V.I.P. System BASE I Processing Specifications* for more information about BASE I STIP functions.

2.5.2 SMS STIP

SMS STIP protects issuer processing capacities and allows issuers to maintain high levels of cardholder service during issuer-unavailable conditions. Risk control options that issuers can specify for STIP include:

- Establishing transaction activity limits for card ranges and for individual cardholders.
- Checking the Exception files for positive account limits (for instance, generous limits for VIP [very important person] accounts) or negative account controls (for instance, card pickup).
- Checking the CVV on the card's magnetic stripe, the CVV or the iCVV on the card's chip image, or the CAVV.
- Checking PINs and monitoring the number of PIN retries.
- Validating the account number with the Luhn modulus-10 algorithm.
- Ensuring a valid card expiration date.

SMS STIP also handles issuer-generated messages including chargebacks, fee collections and funds disbursements, and text messages for unavailable acquirers.

Refer to the V.I.P. System SMS processing specifications manuals for more information about SMS STIP functions.

2.6 RESPONSE PROCESSING

V.I.P. processes responses it receives from issuer centers before it returns the response messages to the acquirer processing centers. The V.I.P. System:

- Checks the format and content of the response.
- Adds a code to indicate that the response came from the issuer center rather than from STIP.
- Drops the CVV- or iCVV-check result code from the message if it is present.

All responses processed by STIP also contain the code that specifies the source of the response. The code indicates why the request was processed by STIP.

When V.I.P. sends a request to an issuer center, it keeps a copy of the request message and waits the allowable period of time governed by the *Visa Operating Regulations* for a response. If there is no response from the issuer by that time, V.I.P. discards the message and does not send a response to the acquirer.

The Assured Transaction Response (ATR) is a function that ensures that timely responses are returned to all requests for authorization and for reversal of Visa card transactions, and for other card transactions. This function is optional for issuers.

With ATR, when V.I.P. sends a request to an issuer center, it keeps a copy of the request message and sets a timer on receipt of the response. If the issuer processing center does not respond within a specified number of seconds, V.I.P. reroutes the request to STIP for processing.

2.7 LOGGING

After V.I.P. validates the source of the message, the system logs the request. V.I.P. logs each request and response message, along with certain system-processing information, in a system log that it uses to prepare reports, to research problems, and to perform billing functions.

2.8 ADDITIONAL V.I.P. FUNCTIONS

In addition to message processing, V.I.P. performs additional functions to support members, V.I.P., and VisaNet. These functions include:

- Managing the network.
- Managing system tables.
- Managing system databases.
- Reporting.
- Billing.

The following subsections describe these functions.

2.8.1 Managing the Network

V.I.P. supports several types of network management messages that control a center's access to the system. These messages enable a center to do the following:

- Sign on and off the system.
- Respond to test messages.
- Monitor response time and connectivity.
- Request advices, and optionally, accelerate advice delivery.
- Enter and exit Suppress Inquiries (SI) Mode. SI Mode is an issuer center station status that blocks all routine incoming authorization and reversal requests during heavy traffic periods.

V.I.P. also creates administrative messages to alert center stations to abnormal system conditions. All administrative messages require the attention of center staff. Upon receipt, they should be routed to a console or to a terminal for immediate review.

Refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals for more information about network management functions.

2.8.2 Managing System Tables

V.I.P. maintains records of member- and Visa-established routing and processing rules that apply to BINs, to processing centers, and to stations. V.I.P. stores these parameters in the system tables (formerly called the system globals).

The system tables are maintained by Visa and are used by BASE I and by SMS. The set of tables contain the following information:

- System parameters
- Lists of valid BINs
- Ranges of valid card numbers
- Center-selected processing parameters
- Member-selected processing parameters such as those an issuer specifies for stand-in processing
- Station-specific parameters such as the types of messages processed (BASE I, SMS, or both) and the message format used

For a detailed discussion of the system tables, refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals.

2.8.3 Managing System Databases

Members supply cardholder and merchant information to V.I.P. for the system to use when it processes request messages. Members also add, change, and delete this information, as needed, to reflect business changes.

Members report any changes in account number ranges or in processing center designations to Visa. This information is vital to the correct routing of messages. Members can both update the files they maintain and request the data from records in those files. Depending on the services selected by the member, V.I.P. can also update information in database files automatically at the time of the transaction.

System databases include:

- Cardholder Database (one for BASE I and one for SMS).
- Merchant Central File.

Issuer centers can update the Cardholder Database files. Acquirer centers can update the Merchant Central File. Members can update files in any of the following ways:

- Using online file update messages for individual updates
- Transmitting a batch file of updates to the VIC through a VisaNet Access Point (VAP) that supports Batch File Update Processing (BFUP)
- Shipping a Center Update Tape (CUP) with a batch of updates to the VIC
- Calling the Visa Service Center with requests for urgent updates
- Submitting the VisaNet Data Capture Profile

Issuer and acquirer centers use online messages to request individual records in any of their files.

Refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals for more information about processing options, limits, and parameters. Members can contact their Visa representatives to select available options and to establish limits and parameters.

2.8.3.1 Cardholder Database Files

The Cardholder Database (CDB) comprises files maintained by Visa, by the issuer, or by both, and resides at each VIC. Both BASE I and SMS have a Cardholder Database. The CDB contains cardholder information used by STIP to authorize transactions and to verify

accounts, addresses, telecodes, and PINs. STIP uses the database to store advices until they are retrieved by issuers.

The database also contains Positive Cardholder Authorization Service (PCAS) and Positive Authorization Capacity Management (PACM) Service limits for individual cardholders.

While card issuers are responsible for creating and for maintaining several of the Cardholder Database files, Visa is responsible for the integrity of these and all V.I.P. system files.

The Cardholder Database contains the following files:

Activity File—This Visa-generated file contains accumulated counts and amounts of Visa-approved transactions and can include accumulated totals of issuer-approved transactions as well as the count of consecutive invalid PIN entries accumulated by STIP.

Address Verification File—This issuer-created and maintained file contains cardholder billing address data.

Advice File—This Visa-generated file contains STIP processing records informing issuers of STIP decisions made on their behalf for authorizations, for verification-only requests, or for reversals.

Exception File—This issuer-created and maintained file contains both positive and negative action codes and other special instructions that indicate that the cardholder's account requires special attention; for instance, the Exception File might note that STIP must decline all transactions for a certain account. The file is also used to create Cardholder Recovery Bulletins (CRBs). Refer to *V.I.P. System Services, Volume 1*, for information about CRBs and about the optional CRB Service.

Certain Visa services, such as the Chargeback Reduction Service and those provided by the Visa Travel Service Center, automatically add and update records in the Exception File to ensure that accounts are included in CRB listings when appropriate.

Full Authorization File—This issuer-created and maintained file is used by the optional Full Authorization Service and contains the cardholder's daily or monthly open-to-use allowances (spending limits) for cash and non-cash transactions. Refer to *V.I.P. System Services, Volume 2*, for information about the Full Authorization Service.

PIN Verification File—This issuer-created and maintained file is used by the optional PIN Verification Service (PVS) and contains Visa PIN Verification Values (PVVs) and PIN Verification Key Indexes (PVKIs) for issuers that use the Visa PVV method of PIN verification. Refer to *V.I.P. System Services, Volume 2*, for information about the PIN Verification Service.

Risk Level File—This issuer-created and maintained file is used for assigning and maintaining individual cardholder's risk levels, daily spending limits, and merchant group daily activity limits. Refer to Part 3 of *V.I.P. System Services, Volume 1*, for information about risk management services.

Telecode Verification File—This issuer-created and maintained file is used for telecode verification and contains cardholders' 4-digit telecodes for the VisaPhone Calling Card Service. Refer to *V.I.P. System Services, Volume 2*, for information about the VisaPhone Service.

Restricted Card List File—MasterCard generates and maintains this file. It contains MasterCard account numbers requiring card pickup. STIP uses this file for MasterCard authorization requests when they cannot be delivered to issuers connected to the MasterCard Banknet network.

For a detailed discussion of the Cardholder Database, refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals.

2.8.3.2 Merchant Central File

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

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

Refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals for more information about this database. Refer to the Merchant Central File Service (MCFS) chapter of *V.I.P. System Services, Volume 2*, for information regarding both the Merchant Central File and MCFS.

2.8.4 Reporting

The V.I.P. reporting components generate various reports available to issuers and to acquirers by subscription. These reports describe V.I.P. processing activity and include information about cardholder listings in the Exception and Advice files. V.I.P. also produces POS and downgraded transaction reports for acquirers. These reports provide individual transaction and summary information. In addition, issuers and acquirers can subscribe to certain reports in raw data file format.

Refer to *V.I.P. System Reports* for report information, including samples. For VisaNet Settlement Service (VSS) report samples, refer to *VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports*.

2.8.4.1 BASE I Reports

The authorization component of the V.I.P. System produces several reports, including:

- Authorization Profile reports (APRs).
- Cardholder Database reports.
- Visa Point-of-Sale reports.
- Custom Payment Service (CPS) reports.

These reports are available to SMS acquirers and issuers by subscription. APRs and Visa Point-of-Sale reports are available in raw data format.

2.8.4.2 Settlement Reports

Issuers and acquirers may also receive the following settlement reports:

- VisaNet Settlement Service (VSS) reports
- International Settlement Service reports
- National Net Settlement Service reports

For further information on settlement reports, refer to *VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports*.

2.8.4.3 Raw Data Records

SMS participants can choose to receive raw data records that detail member transaction activity for the processing day. Raw data allows members to analyze and to customize their data in the way that best suits their business needs. For more information about raw data, see *VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports*.

BASE I participants can also receive raw data. For details, refer to *V.I.P. System BASE I Technical Specifications*.

2.8.5 Billing

Visa assesses the fees and charges for V.I.P. processing on a monthly basis. V.I.P. produces printed invoices that provide the line-item detail of costs for accessing the system, for routing and processing messages, for maintaining files, and for creating reports. At the member's request, V.I.P. prepares invoices either for individual BINs or for an entire processing center, which then bills its own users. Members can contact their Visa representatives to find out more about V.I.P. billing.

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 3

V.I.P. System Services

The V.I.P. System provides many services beyond its basic functionality. Some services are mandatory for all members or for members in specific Visa regions, but most services are optional. Members can subscribe to optional V.I.P. services anytime.

Service enrollment processes differ for each region. Before any service implementation, each member must test its systems and, in many cases, become certified by Visa to implement the service. Visa representatives can explain the regional requirements and enrollment specifics.

This chapter summarizes the services available to BASE I members, to Single Message System (SMS) members, or to both. Refer to *V.I.P. System Services, Volume 1 and Volume 2*, for complete service descriptions. See also *V.I.P. System BASE I Processing Specifications* and the V.I.P. System SMS processing specifications manuals for information about services not yet included in *V.I.P. System Services*.

3.1 SERVICE FUNCTIONAL GROUPS

V.I.P. services can be categorized into the following groups by service function:

- Routing Services
- Risk Management Services
- Visa Secure Electronic Commerce (VSEC) Services
- Chip Card Services
- Authorization Database Services
- Authorization Services

Table 3-1 lists V.I.P. services by functional group.

Table 3-1 V.I.P. Services by Functional Group

Functional Group	Services
Routing	ATM/POS Split Routing Service
	Check Acceptance Service
	Gateway Services
	Integrated Debit Service
	PIN/No-PIN Split Routing Service
	Priority Routing Service
	Visa Shortest Online Path (VSOP) Service
Risk Management	Card Recovery Bulletin (CRB) Service
	Fraud Reporting System (FRS)
	Visa Issuer Fraud Detection (VIFD) Service

Table 3-1 V.I.P. Services by Functional Group (continued)

Functional Group	Services
Visa Secure Electronic Commerce (VSEC)	Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)
Chip Card	Visa Cash CEPS Service Visa Horizon Service Visa Smart Debit/Smart Credit (VSDC) Service
Authorization Database	Automatic Cardholder Database Update (Auto-CDB) Service Merchant Central File Service (MCFS)

Table 3-1 V.I.P. Services by Functional Group (continued)

Functional Group	Services
Authorization	Account Verification Service
	Address Verification Service (AVS)
	Advanced Authorization Service
	Advice Retrieval Service—BASE I
	Advice Retrieval Service—SMS
	ATM Format Conversion Service
	Card Verification Value (CVV) Service
	Card Verification Value 2 (CVV2) Service
	Cardholder Authentication Verification Value (CAVV) Verification Service
	Custom Payment Service (CPS)/ATM
	Custom Payment Service (CPS)/POS
	Deferred Clearing Advice File (DCAF) Service
	Dynamic Key Exchange (DKE) Service
	Full Authorization Service
	International Automated Referral Service (IARS)
	Multicurrency Service
	PIN Verification Service (PVS)
	POS Check Service
	Positive Authorization Capacity Management (PACM) Service
	Positive Cardholder Authorization Service (PCAS)
	Preauthorized Payment Cancellation Service (PPCS)
	Status Check Service
	Visa Cashback Service
	VisaPhone Service

Table 3-1 V.I.P. Services by Functional Group (continued)

Functional Group	Services
Additional	Chargeback Reduction Service (CRS)
	Visa check card II
	ATM Processing Integration

3.2 ROUTING SERVICE DEFINITIONS

This section provides basic definitions of V.I.P. routing services. Refer to *V.I.P. System Services, Volume 1*, for complete service descriptions.

3.2.1 ATM/POS Split Routing Service

The ATM/POS Split Routing Service enables BASE I and SMS issuers that process Visa, Visa Electron, and Plus transactions to use separate processing centers for ATM transactions and for POS transactions. This service offers the following options:

ATM Account-Type Split Routing—The ATM Account-Type Split Routing option is available for BASE I and SMS issuers that process ATM transactions. Issuers can specify that VisaNet route ATM transactions based on the account the cardholder selects when using a multipurpose card at an ATM. Issuers can specify up to three endpoints: one for deposit accounts, one for credit accounts, and one for universal and non-specified accounts.

Alternate Routing—With the Alternate Routing option, acquirers and issuers can designate one or two alternate processing centers to handle exception and other back office transactions. The alternate processing center may be connected to the SMS component of the V.I.P. System or to the Visa BackOffice Adjustment System (BOAS).

Issuers can use these routing options separately or in combination.

3.2.2 Check Acceptance Service

The Check Acceptance Service allows merchants in the United States (U.S.) region to route check approval requests through VisaNet to selected check acceptance vendors. One of five companies, Equifax Card Services (TeleCredit Los Angeles and TeleCredit Tampa), ETC Scan (Delux Data Systems), JBS/NPC, State Street Bank, or TeleCheck, can approve a check used at a merchant location through the Check Acceptance Service. The vendor guarantees acceptance of the check by the drawee bank and assumes responsibility for collection if the check is returned.

3.2.3 Gateway Services

Both the BASE I component and the SMS component of the V.I.P. System have connections, or *gateways*, to various other systems and networks. Gateway Services enable acquirers to obtain authorizations on non-Visa-brand transactions through the same VisaNet connections they use for Visa transactions. With Gateway Services, acquirers and merchants can route all terminal traffic to V.I.P., which then routes non-Visa-brand transactions to the appropriate networks for responses. The service also enables issuers to use their V.I.P. System links to receive requests from other networks or services.

3.2.4 Integrated Debit Service

The Integrated Debit Service enables merchants in the U.S. region to accept customer payments made with debit cards and ATM cards bearing a national or regional debit point-of-sale (POS) mark. Merchants send transactions initiated with these cards (and accessed with personal identification numbers [PINs]) to the V.I.P. System. The SMS component of V.I.P. routes these transactions through the VisaNet Debit gateway to the appropriate direct-debit POS network for delivery to the issuer.

Routing options provide merchants with flexibility in accessing the various debit POS networks, which, in turn, route transactions to the issuers.

The Integrated Debit Service also supports Electronic Benefits Transfer (EBT), a federally sponsored program. EBT is a nationwide program of card-accessed, electronically delivered, government-funded benefits that are issued through a federal-state partnership. The primary function of EBT, as it exists today, is the electronic delivery of food stamps and cash benefits.

3.2.5 PIN/No-PIN Split Routing Service

The PIN/No-PIN Split Routing Service allows issuers to separate transactions requiring PIN verification from those that do not and to route these transactions to two or more issuer processing centers. The service offers the following options:

- PIN Routing option for routing all POS financial transactions with PINs to SMS and all other transactions to BASE I.
- The Alternate Routing option for separating original transactions and exception transactions.

Issuers can use these split routing options individually or in combination.

3.2.6 Priority Routing Service

The Priority Routing Service determines the destination of authorization, financial, and reversal requests based on the acquirer's processing order preference. The service is available for SMS acquirers.

To initiate the Priority Routing Service, acquirers specify network ID 0000 in the request, allowing VisaNet to determine which network and card program rules apply based on the account number and on acquirer-provided preferences.

The acquirer assigns processing priorities to each of its card programs. By setting up a preferred processing path, acquirers can choose how a transaction that qualifies for more than one card program should be processed.

3.2.7 Visa Shortest Online Path (VSOP) Service

The Visa Shortest Online Path (VSOP) Service allows non-U.S. issuers that issue both Visa and MasterCard card products to receive MasterCard authorization requests for purchase and cash transactions acquired through VisaNet. This service foregoes the need to route MasterCard requests to BankNet (the MasterCard processing network) before they go to the issuer.

The VSOP Service operates only when the issuer is available to authorize the MasterCard transaction. Otherwise, V.I.P. routes the transaction to stand-in processing (STIP) or to MasterCard through Gateway Services.

3.3 ROUTING SERVICE AVAILABILITY

Specific routing services are available for BASE I and SMS acquirers and issuers. Table 3-2 lists the systems and products and the corresponding routing services available.

Table 3-2 Routing Service Availability

	AVAILABLE FOR...				
Routing Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**	**Products**
ATM/POS Split Routing Service	✓	✓	✓	✓	Visa Electron, Interlink, Plus, Visa
Check Acceptance Service	✓		✓	✓	Available for checks
Gateway Services	✓		✓	✓	Available for all product types
Integrated Debit Service	✓	✓		✓	Available for all product types
PIN/No-PIN Split Routing Service	✓	✓	✓	✓	Visa Electron, Interlink, Plus, Visa
Priority Routing Service	✓			✓	Visa Electron, Interlink, Plus ATM, Visa
Visa Shortest Online Path (VSOP) Service		✓	✓		MasterCard

3.4 RISK MANAGEMENT SERVICE DEFINITIONS

This section provides basic definitions of the fraud risk reduction services provided through V.I.P. Refer to *V.I.P. System Services, Volume 1*, for complete service descriptions.

3.4.1 Card Recovery Bulletin (CRB) Service

The Card Recovery Bulletin (CRB) Service is an international risk control service that publishes bulletins and card recovery files containing account numbers of cards reported as lost, stolen, or misused. It publishes Card Recovery Bulletins (paper bulletins) for non-U.S. issuers and acquirers, maintains card recovery files (including the CD-ROM bulletin) for most acquirers, and merchant mailing files for all acquirers. The service also helps control fraud on below-floor-limit transactions outside the U.S.

The CRB Service assures that cardholders are protected from fraudulent use of their lost or stolen cards. It also supports chargeback rights of issuers, acquirers, merchants, and cardholders.

BASE I and SMS issuers can list Visa account numbers in the BASE I Exception File, coded to appear in specified bulletins and pickup files. The BASE I Exception File is the only source of Exception File input for the CRB. SMS issuer participants must list their accounts in *both* the BASE I and SMS Exception files so that the account listings are included in the CRB.

An issuer can elect to list an account number in one or more individual CRB regions, or in a combination of individual regions plus one or more groups of regions. Visa acquirers specify

which regional bulletins go to which merchant locations, and which bulletins, pickup files, or both, they want sent to themselves or to their processing centers.

3.4.2 Fraud Reporting System (FRS)

The Fraud Reporting System (FRS) is available as a V.I.P. service to help members report, track, and analyze fraudulent transactions. FRS consolidates fraud information, helping members detect fraud patterns and reduce losses.

3.4.3 Visa Issuer Fraud Detection (VIFD) Service

The Visa Issuer Fraud Detection (VIFD) Service is an authorization scoring and reporting service that utilizes advanced technologies, consisting of statistical models and neural networks, to identify fraud patterns and to score individual transactions processed through VisaNet.

VIFD is designed to reduce issuer fraud within the U.S. region. When an authorization is scored above a threshold established by the issuer, VIFD generates an alert for the account. VIFD enables issuers to detect fraud much earlier than is normally possible with in-house fraud detection systems.

3.5 RISK MANAGEMENT SERVICE AVAILABILITY

Specific risk management services are available for BASE I and SMS acquirers and issuers. Table 3-3lists the systems and the corresponding risk management services available.

Table 3-3 Risk Management Service Availability

	AVAILABLE FOR...			
Risk Management Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**
Card Recovery Bulletin (CRB) Service	✓	✓	✓	✓
Fraud Reporting System (FRS)[1]	✓	✓		✓
Visa Issuer Fraud Detection (VIFD) Service		✓	✓	✓

1. FRS is available to BASE I participants through TC 40 BASE II records.

3.6 VISA SECURE ELECTRONIC COMMERCE (VSEC) SERVICE DEFINITION

This section gives a basic definition of the VSEC service provided through V.I.P. Refer to *V.I.P. System Services, Volume 1*, for a complete service description.

3.6.1 Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)

The Visa Secure Electronic Commerce (VSEC) initiative provides security for transactions sent over the Internet and other open networks. Implemented as part of the VSEC initiative, Visa has developed technology to authenticate the cardholder during an online purchase. The *authentication technology* is called 3-D Secure; the *authentication service* available to cardholders is referred to as Verified by Visa.

Verified by Visa gives cardholders control over card use for online purchases and provides payment security that adds an extra level of protection both for consumers and for merchants.

Verified by Visa enables all parties in an electronic commerce (e-commerce) payment transaction to transmit confidential payment data and provides authentication that the buyer is

an authorized user of a particular account. Verified by Visa is a global program that supports both magnetic stripe Visa cards and Visa Smart Debit and Smart Credit (VSDC) cards.

VisaNet validates the results of authentication during authorization. See the "Cardholder Authentication Verification Value (CAVV) Verification Service" section of this chapter for more information about the CAVV Verification Service.

3.7 VSEC SERVICE AVAILABILITY

VSEC services are available to BASE I and SMS acquirers and issuers. Table 3-4lists the systems and service availability.

Table 3-4 VSEC Service Availability

	AVAILABLE FOR...			
VSEC Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**
Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)	✓	✓	✓	✓

3.8 CHIP CARD SERVICE DEFINITIONS

This section provides basic definitions of the chip card services provided through V.I.P. Refer to *V.I.P. System Services, Volume 1*, for complete service descriptions.

3.8.1 Visa Cash CEPS Service

Visa Cash is a global chip-based card that offers consumers a fast and convenient method of making small-ticket (under US$10) purchases. Based on the Common Electronic Purse Specification (CEPS), Visa Cash CEPS is designed to replace currency and coins for small-ticket cash transactions, such as for a cup of coffee, newspaper, phone call, or public transportation ticket, at merchant locations that do not usually accept checks or traditional bank cards.

3.8.2 Visa Horizon Service

The Visa Horizon Service enables cardholders to use a single-currency payment Visa Horizon card, based on Chip Offline Pre-Authorized Card (COPAC) and integrated-circuit technologies, that contains preauthorized spending power for purchases or cash disbursements. Unlike stored value cards, this spending power is linked to collateral funds that are held either in the cardholder's source account or in a separate "shadow account." Funds are not deducted from those collateral funds until financial transactions have been successfully cleared and settled.

Cardholders initiate Visa Horizon transactions by inserting a Visa Horizon card in an appropriate terminal and entering a PIN. Visa Horizon cards can also be used at Visa Smart Debit and Smart Credit (VSDC) terminals displaying the Visa Horizon mark.

3.8.3 Visa Smart Debit/Smart Credit (VSDC) Service

The Visa Smart Debit/Smart Credit (VSDC) Service provides members with a safe and controlled means to incorporate credit and debit functionality into chip cards. VSDC is a debit or credit service that takes full advantage of the power of the microchip on a single card. VSDC supports Visa, Visa Electron, and Plus card products.

Chip Card Service Availability

The VSDC baseline product, the chip card, provides all debit and credit functions currently available in a magnetic stripe product; it also has additional features that allow issuers to customize their products to accommodate their market strategy and their customers' needs.

Whenever a cardholder uses a VSDC card at a chip-capable terminal, the interaction between card and terminal provides new transaction security and functionality. Based on issuer-selected features, the card and terminal interaction results in a payment transaction similar to that performed with today's magnetic stripe cards. However, with the VSDC Service, the card and terminal interaction can provide a suite of optional risk control features. Issuers can activate any or all of these features during the card personalization process when they put account information on the chip.

3.9 CHIP CARD SERVICE AVAILABILITY

Specific chip card services are available for BASE I and SMS acquirers and issuers. Table 3-5lists the systems and the corresponding chip card services available.

Table 3-5 Chip Card Service Availability

	AVAILABLE FOR...			
Chip Card Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**
Visa Cash CEPS Service	✓	✓	✓	✓
Visa Horizon Service	✓	✓	✓	
VSDC Service	✓	✓	✓	✓

3.10 AUTHORIZATION DATABASE SERVICE DEFINITIONS

This section provides basic definitions of V.I.P. services that members can use to update their information in the two main V.I.P. system databases:

- Cardholder Database
- Merchant Central File

Chapter 2, V.I.P. Transaction Processing, discusses these two system database files. Refer to *V.I.P. System Services, Volume 2*, for complete service descriptions.

3.10.1 Automatic Cardholder Database Update (Auto-CDB) Service

The Automatic Cardholder Database Update (Auto-CDB) Service enables BASE I and SMS issuers to update the BASE I and SMS Exception files, contained in the Cardholder Database, as part of their authorization response messages. The BASE I and SMS Exception files are separate and are updated individually.

The Auto-CDB Service helps issuers prevent losses from problem accounts by improving the accuracy of cardholder information available to V.I.P. for stand-in processing.

3.10.2 Merchant Central File Service (MCFS)

The Merchant Central File Service (MCFS) supplies information from the Merchant Central File, a database created and maintained by acquirers.

The Merchant Central File is a VIC-resident file that acquirers use to store BASE I authorization or reversal request information that cannot otherwise be supplied by a terminal at the point of sale or the point of service (POS) because of device limitations.

MCFS adds the information from the Merchant Central File (if the data is available) before forwarding the request to the issuer or to STIP.

3.11 AUTHORIZATION DATABASE SERVICE AVAILABILITY

Specific authorization database services are available to BASE I and SMS acquirers and issuers. Table 3-6lists the systems and the corresponding authorization database services available.

Table 3-6 Authorization Database Service Availability

	AVAILABLE FOR...			
Authorization Database Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**
Automatic Cardholder Database Update (Auto-CDB) Service		✓	✓	✓
Merchant Central File Service (MCFS)	✓		✓	

3.12 AUTHORIZATION SERVICE DEFINITIONS

This section provides basic definitions of V.I.P. authorization services. Refer to *V.I.P. System Services, Volume 2*, for complete service descriptions.

3.12.1 Account Verification Service

The Account Verification Service enables merchants to request an account number verification as an initial check for an estimated purchase.

Using an authorization request message, merchants can request:

- Account verification only, to perform an initial check for an estimated purchase.
- Account verification and authorization, to request authorization when the transaction takes place at the POS.

The service replaces the manual process of checking paper Card Recovery Bulletins (CRBs). Instead of using a paper bulletin, the merchant contacts its acquirer to initiate an account verification request.

3.12.2 Address Verification Service (AVS)

The Address Verification Service(AVS) is an online Visa service that enables merchants in all Visa regions to reduce fraud losses by verifying cardholders' billing addresses for card-not-present transactions.

AVS can be used for Visa, MasterCard, American Express, and Discover transactions.

3.12.3 Advanced Authorization Service

Advanced Authorization Service improves the authorization process by supplying issuers with transaction risk assessments. These account number-based assessments are performed online when the authorization request reaches V.I.P. V.I.P. inserts fields containing the results of this analysis in the request as it is forwarded to the issuer. Only U.S. issuers receive this information; it is currently not sent to acquirers or to merchants.

Advanced Authorization risk scoring applies to all U.S.-issued Visa cards used in POS and in ATM authorization requests. The service does not apply to Check Acceptance, Visa Cash, or PIN change/block/unblock transactions.

Acquirers and merchants do not have to be in the U.S. U.S. issuers must participate and must be certified for the fields. Field 62.21 is required. Issuers can elect to also receive field 62.22.

3.12.4 Advice Retrieval Service—BASE I

The BASE I Advice Retrieval Service keeps issuers informed of stand-in authorizations, reversals, and Cardholder Database file updates by allowing issuers to retrieve their advice data from the BASE I Advice File at their VisaNet Interchange Center (VIC).

Each VIC maintains a BASE I Advice File, in which it stores BASE I STIP response records. Every record contains information from the authorization or reversal request, the STIP response, and the reason why STIP processed the request.

3.12.5 Advice Retrieval Service—SMS

The SMS Advice Retrieval Service keeps issuers informed of stand-in authorizations, reversals, deferred clearing advices, and SMS Exception File updates by allowing members to retrieve their advice data from the SMS Advice File at their VIC.

Each VIC maintains an SMS Advice File in which it stores SMS STIP response records. Each record contains information from the authorization or reversal request, the STIP response, and the reason why STIP processed the request.

3.12.6 ATM Format Conversion Service

The ATM Format Conversion Service provides Visa and Visa Electron SMS issuers, including those co-branded with Plus, with the option to receive eligible ATM transactions from dual-message acquirers as full financial messages.

NOTE

V.I.P. always delivers ATM transactions for proprietary cards with the Plus mark to SMS issuers as full financial messages regardless of the method by which they were acquired.

3.12.7 Card Verification Value (CVV) Service

The Card Verification Value (CVV) Service is a POS and ATM risk control service that protects issuers and acquirers from fraud losses associated with counterfeit Visa cards. The CVV Service allows issuers to detect invalid cards by validating the CVV on the physical magnetic stripe of the cards, and the CVV or the Integrated Chip Card Verification Value (iCVV) on the magnetic stripe image on the chip.

The CVV or iCVV is a unique value calculated from magnetic stripe data using a Data Encryption Standard (DES) algorithm established by Visa. V.I.P. or the issuer can perform CVV or iCVV calculations when both the issuer and the acquirer are participating in the service and the magnetic stripe data is transmitted.

3.12.8 Card Verification Value 2 (CVV2) Service

The Card Verification Value 2 (CVV2) Service is a card verification tool designed to reduce fraud losses on transactions when the card is not present, and in the Latin America and Caribbean (LAC) region, in certain situations when the card is 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 Operating Regulations*. Members can use the CVV2 number to validate that a genuine Visa card is present at the cardholder location during a

transaction. The CVV2 is calculated using a secure cryptographic process and a key known only to the issuer and to Visa.

3.12.9 Cardholder Authentication Verification Value (CAVV) Verification Service

The Cardholder Authentication Verification Value (CAVV) Verification Service provides the functionality to verify that the Cardholder Authentication Verification Value (CAVV) submitted by an acquirer in a Verified by Visa (3-D Secure) authorization message matches the CAVV generated by the Visa or by an issuer's Access Control Server (ACS) during authentication.

The *CAVV* is a cryptographic value generated by the issuer and sent to the merchant during the authentication process in a Verified by Visa transaction.

The CAVV Verification Service is part of a suite of services available through Verified by Visa. Visa developed Verified by Visa to enhance the security and integrity of Internet purchases made using Visa cards. The service allows issuers to register cardholders for the service and to authenticate the cardholder as the owner of the card account when an online purchase occurs at a participating merchant location. See the "Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)" section of this manual for information about Verified by Visa.

3.12.10 Custom Payment Service (CPS)/ATM

Custom Payment Service (CPS)/ATM is an incentive program that provides accurate settlement and improved management of the cardholder's accounts through better matching of messages, from authorization through clearing, using a unique transaction identifier.

In addition, CPS/ATM ensures more timely delivery of clearing records by acquirers and reduces exception item processing by improving transaction integrity and life-cycle control.

3.12.11 Custom Payment Service (CPS)/POS

Custom Payment Service (CPS)/POS is a series of payment services that are customized to serve the needs of distinct merchant segments for point-of-sale (POS) transactions. CPS/POS accommodates different merchant procedures, and decreases fraud losses and operating expenses associated with each transaction. CPS/POS increases Visa member profitability by reducing member operating costs, improving risk management techniques, and increasing member revenues through increased card usage.

CPS/POS transactions can be processed as dual messages through BASE I and BASE II.

3.12.12 Deferred Clearing Advice File (DCAF) Service

The Deferred Clearing Advice File (DCAF) Service allows members processing in a single-message environment to receive original BASE II deferred clearing advices in bulk file deliveries.

BASE II deferred clearing advices originate from dual-message acquirers that do not generate online clearing messages. Without the DCAF Service, 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.

3.12.13 Dynamic Key Exchange (DKE) Service

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

3.12.14 Full Authorization Service

Full Authorization Service is an extension of V.I.P. stand-in processing. This service allows issuers to specify cardholder daily and monthly spending limits in addition to limits already established for STIP. This ability to specify limits enables issuers to tightly control and track total cardholder activity and authorizations against issuer-specified limits.

3.12.15 International Automated Referral Service (IARS)

The International Automated Referral Service (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.

3.12.16 Multicurrency Service

The Multicurrency Service allows members to authorize and to settle transactions in any nominated currency. The service supports authorization, clearing, and settlement processing in selected international currencies.

3.12.17 PIN Verification Service (PVS)

The PIN Verification Service (PVS) is a V.I.P. service that provides full-time or stand-in verification of personal identification numbers (PINs) used for Visa and Plus ATM transactions, for Visa point of service (POS), Visa Electron POS, and Interlink POS transactions, and for Visa Smart Debit/Smart Credit (VSDC) transactions. A *personal identification number* is a secret code that identifies a cardholder at an ATM or a terminal. 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 to the V.I.P. stand-in processor (STIP), as appropriate, for authorization processing.

3.12.18 POS Check Service

The POS Check Service offers merchants the ability to accept consumer and business checks as source documents and to convert the paper checks to electronic transactions at the point of sale, and from mail, telephone, or electronic commerce merchants. As electronic transactions, converted checks can be cleared and settled quickly and efficiently. Merchants using this service can realize the benefits of cost and risk reduction for check payments. Participating drawee financial institutions, serving as online authorizing agents for their customers' checks, can clear and settle electronic debits quickly, increasing revenue opportunities and reducing check processing costs.

3.12.19 Positive Authorization Capacity Management (PACM) Service

The Positive Authorization Capacity Management (PACM) Service helps BASE I and SMS issuers maximize their authorization and full financial message processing capacity.

PACM monitors the issuer's transaction volume every 60 seconds. 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.

3.12.20 Positive Cardholder Authorization Service (PCAS)

The Positive Cardholder Authorization Service (PCAS) is a comprehensive set of risk control parameters available to BASE I issuers that determine whether an authorization request is switched to the issuer or is processed by STIP.

If the transaction is routed to the issuer, the issuer provides the response. If the transaction is routed to STIP, V.I.P. provides the response based on stand-in authorization options and on PCAS processing limits. Issuers can choose from a variety of options that either increase authorization risk control or customer service levels, or control authorization expenses. These parameters are flexible and can be customized by merchant type, cardholder risk level, and cardholder spending.

3.12.21 Preauthorized Payment Cancellation Service (PPCS)

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

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

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

The Preauthorized Payment Cancellation Service (PPCS) can be used both by BASE I and by SMS users.

3.12.22 Status Check Service

A status check request is an authorization request for one unit of currency (such as one U.S. dollar). Merchants use this type of authorization request to verify the customer's account status when the final transaction amount is not yet known, such as when a customer checks into a hotel. V.I.P. forwards status check requests directly to the issuer when the issuer is available, bypassing STIP.

The Status Check Service allows merchants such as hotels, auto rental companies, the U.S. VisaPhone program, and the Global Customer Assistance Service (GCAS), to receive authorizations without the issuer reducing cardholders' open-to-buy amounts. The Status Check Service is also available for automated fuel dispenser merchants.

3.12.23 Visa Cashback Service

The Visa Cashback Service is a domestic service available as an option to participating Visa regions for their issuers, acquirers, and merchants on all Visa Flag, Visa Electron, and Visa Horizon products. *Cash back* is defined as cash given to the cardholder at the point of sale when a purchase is made.

Acquirers and issuers must be certified in the service to participate. Participating regions and countries within those regions establish maximum cashback amounts.

3.12.24 VisaPhone Service

The VisaPhone Service allows cardholders to use their Visa cards as calling cards while traveling. VisaPhone calls are automatically billed to the cardholder's Visa account.

3.13 AUTHORIZATION SERVICE AVAILABILITY

Specific authorization services are available for BASE I and SMS acquirers and issuers. Table 3-7lists the systems and the corresponding authorization services available.

Table 3-7 Authorization Service Availability

	AVAILABLE FOR...			
Authorization Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**
Account Verification Service	✓		✓	✓
Address Verification Service (AVS)	✓	✓	✓	✓
Advanced Authorization Service		✓	✓	✓
Advice Retrieval Service—BASE I		✓	✓	
Advice Retrieval Service—SMS	✓	✓		✓
ATM Format Conversion Service		✓		✓
Card Verification Value (CVV) Service	✓	✓	✓	✓
Card Verification Value 2 (CVV2) Service	✓	✓	✓	✓
Cardholder Authentication Verification Value (CAVV) Verification Service	✓	✓	✓	✓
Custom Payment Service (CPS)/ATM	✓	✓	✓	
Custom Payment Service (CPS)/POS	✓	✓	✓	
Deferred Clearing Advice File (DCAF) Service		✓		✓
Dynamic Key Exchange (DKE) Service	✓	✓		✓
Full Authorization Service		✓	✓	
International Automated Referral Service (IARS)	✓	✓	✓	✓
Multicurrency Service	✓	✓	✓	✓
PIN Verification Service (PVS)		✓	✓	✓
POS Check Service	✓	✓		✓
Positive Authorization Capacity Management (PACM) Service		✓	✓	✓
Positive Cardholder Authorization Service (PCAS)		✓	✓	
Preauthorized Payment Cancellation Service (PPCS)	✓	✓	✓	✓

Table 3-7 Authorization Service Availability (continued)

	AVAILABLE FOR...			
Authorization Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**
Status Check Service	✓	✓	✓	
Visa Cashback Service	✓	✓	✓	✓
VisaPhone Service	✓	✓	✓	

3.14 ADDITIONAL SERVICE DEFINITIONS

This section provides basic definitions of additional services available through V.I.P. Refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. SMS processing specifications manuals for more information. These services will be documented in future updates of *V.I.P. System Services*, if appropriate.

3.14.1 Chargeback Reduction Service (CRS)

The VisaNet Chargeback Reduction Service (CRS) is designed to help:

- Reduce member costs by eliminating unnecessary exception items (chargebacks, copy requests, and representments).
- Improve the accuracy and the timeliness of valid exception transactions.

CRS applies to Visa and Visa Electron POS transactions only, and not to ATM or Interlink transactions.

3.14.2 Visa Check Card II

Visa check card II is a U.S.-domestic service that allows a cardholder to use a debit account for POS and ATM transactions. Visa check card II transactions can be signature- or PIN-based, and can include cash back for acquirers participating in the cashback program.

Issuers must establish a separate BIN for Visa check card II accounts and must support PIN processing as well as cashback transactions. PIN and cashback processing support are optional for acquirers.

3.14.3 ATM Processing Integration

SMS participants that want to format and process *all* ATM transactions without distinguishing between Visa ATM and Plus ATM transactions can do so by changing the coding for specific fields. For more information, refer to the V.I.P. System SMS processing specifications manuals.

3.15 ADDITIONAL SERVICE AVAILABILITY

Specific additional services are available for BASE I and SMS acquirers and issuers. Table 3-8lists the systems and the corresponding additional services available. These services will be documented in future updates of *V.I.P. System Services*, if appropriate.

Additional Service Availability

Table 3-8 Additional Service Availability

	AVAILABLE FOR...			
Additional Service	**Acquirer**	**Issuer**	**BASE I**	**SMS**
Chargeback Reduction Service (CRS)	✓	✓		✓
Visa Check Card II	✓	✓	✓	✓
ATM Processing Integration	✓	✓		✓

THIS PAGE INTENTIONALLY LEFT BLANK.

Chapter 4

Acquirer and Issuer Responsibilities

This chapter outlines the responsibilities and options for acquirers and issuers that want to connect to the V.I.P. System. All members must first establish a processing center. Each processing center must then fulfill the responsibilities specific to acquirers and to issuers.

4.1 ESTABLISHING PROCESSING CENTERS

Acquirers and issuers mustestablish an in-house processing center or designate another center or third-party processor to perform the necessary processing functions. The processing center needs to have the systems necessary to supply merchant support services, cardholder support services, or both. Support services include the ability to communicate with the merchant sites and with cardholders, as well as with V.I.P., at the VisaNet Interchange Center (VIC).

4.1.1 Network Stations

A single processing center can have any number of physical network stations in VisaNet, based on volume and on business needs.

Acquirers and issuers can establish multiple network stations to:

- Handle a high volume of traffic.
- Process BASE I and Single Message System (SMS) traffic separately.
- Accommodate multiple acquirer business locations.

The following examples describe situations in which multiple business locations are necessary.

EXAMPLE

An acquirer or an issuer could operate multiple in-house stations at one processing center.

EXAMPLE

An issuer could operate an in-house center with one or more stations to process its cardholders' purchase transactions and could contract with another center to handle its ATM business with personal identification numbers (PINs).

EXAMPLE

An acquirer could sponsor a major merchant center with one or more stations, and could operate an in-house center with one or more stations to serve its other merchants and its own business locations.

EXAMPLE

An acquirer or an issuer could operate one or more in-house stations at each of multiple centers.

For more information about network stations, refer to About This Manual for a list of VisaNet Access Point (VAP) documents.

4.1.2 V.I.P. Message Support

The processing center must be capable of generating and receiving all types of V.I.P. messages necessary for the card processing it performs. It must establish access to V.I.P., update system files at the VIC, and provide full message support.

Message support includes the following:

- The ability to generate the appropriate type of message for the function desired.
- The ability to receive all applicable incoming messages.
- The ability to supply data required in the V.I.P. request when it is not available from the point of sale or point of service (POS). Acquirer processing centers optionally can use the Merchant Central File Service (MCFS) to perform this task.
- The ability to manage all of the messages related to any given customer transaction. This management is critical to V.I.P. processing. Acquirers and issuers must avoid duplicate postings and must accurately calculate settlement totals.
- Support for any optional system service or feature used, for instance, the Full Authorization Service or the Merchant Central File Service (MCFS). Refer to *V.I.P. System Services* for details of individual service requirements.
- Downtime procedures and appropriate recovery measures.

The V.I.P. message format provides enhanced processing capabilities to members and to processors. All centers, BASE I or SMS, that are connecting to the V.I.P. System for the first time are required to use the V.I.P. message format.

Refer to *V.I.P. System BASE I Technical Specifications* and to the V.I.P. System SMS technical specifications manuals for details about message formats.

4.1.3 Testing and Certification

Visa must test and certify centers' message processing capabilities before they can use the V.I.P. System. During the testing and certification process, the processing center sends and receives test messages. Visa monitors the transactions to ensure that the processing center is able to process all message types correctly. Members can contact their Visa representatives for complete information about testing and certification.

4.1.4 Network Management

Processing centers must be able to control and support the following:

- Center system status. When the center's authorization system is down, it must sign off from VisaNet. If the center has a front-end processor and that processor is down, it must sign off from VisaNet.
- Test messages.
- Advice Recovery mode.
- Other applicable network-related functions, such as BASE I Suppress Inquiries (SI) Mode.

For additional information, refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals.

4.1.5 SMS Reconciliation and Settlement

The V.I.P. System automatically generates reconciliation advices for SMS members. These advices must be received by Visa POS, Visa Electron, Interlink, and ATM acquirers, and also by Visa POS and Interlink issuers.

Processing centers should be able to accumulate *settlement totals*, which are the gross values of transactions processed. If the center processes for several institutions, it should also be able to allocate settlement totals to those institutions.

Processing centers should also be able to find and to resolve settlement discrepancies. Visa assumes that V.I.P. System totals are valid unless disproved by the processing center. Processing centers can use the detailed activity reports to trace transactions and to resolve discrepancies.

In addition, if acquirers or issuers want to use SMS processing, they must make the following decisions:

- Acquirers that participate in multiple networks must decide whether to use the Priority Routing Service. To use the Priority Routing Service, they must establish a network processing priority list for Visa. Refer to *V.I.P. System Services, Volume 1*, for information on this V.I.P. service.
- Whether to act as a settlement entity or to designate one. A *settlement entity* is the clearing agent that establishes an account for funds transfer. This account can be established at the transfer agent used by SMS for settlement or at any institution accessible through the Federal Reserve wire transfer system.

  When acting as a settlement entity and also sponsoring another institution or major merchant, the acquirer is responsible for allocating funds transfer totals. V.I.P. provides settlement reports at various levels for control and for financial accounting but only transfers funds at the settlement entity level. Refer to *V.I.P. System Reports* for a list of available reports and report samples.
- The level of settlement reporting they want from V.I.P.

Refer to the V.I.P. System SMS processing specifications manuals for reconciliation and settlement information.

For further information about settlement considerations, refer to the BASE II and VisaNet Settlement Service (VSS) documents listed in About This Manual.

4.2 ACQUIRER PROCESSING CENTER REQUIREMENTS

The following requirements apply to acquirer processing centers that want to implement V.I.P. card transaction processing:

- POS connections and procedures
- PIN security
- Response procedures
- Merchant Central File management
- Follow-up procedures and processing
- Other responsibilities

The following subsections explain these requirements.

4.2.1 POS Connections and Procedures

The processing center must establish a means of communication between itself and all of the acquirer's points of sale and points of service. To facilitate communication, processing centers install electronic terminals at points of service or provide phone authorization service to merchant sites that only require authorization processing.

Setting up communications facilities involves:

- Establishing and maintaining a merchant network, an ATM network, or both, if applicable. This step is required for most BASE I acquirer centers and for all SMS acquirer centers.

  Acquirer centers are responsible for providing and for maintaining:
  - POS devices.
  - Communications facilities of the network.
  - Merchant operating procedures.
  - Capability to support the request and response messages to and from the POS location.
- Arranging phone service and authorization support for merchant sites and for branch offices, if applicable. This step is required for those BASE I acquirer centers that serve merchant sites without electronic terminals or that provide this service as backup to their network service. Acquirers may choose to contract this type of service from an outside entity.

  When acquirers provide phone authorization service, the acquirer centers are responsible for authorization staff that can:
  - Take calls requesting approvals of card transactions.
  - Make provisions for entering those requests into their own card processing systems.
- Establishing a card processing system that can accept and can respond to requests from the POS network, from the ATM network, or from both, or establishing an in-house authorization center.

In addition, acquirers must establish POS procedures using merchant agreements. These agreements must determine the following:

- The rules and the parameters for card acceptance, such as merchant floor limits.
- Processing charges and merchant discounts.
- Authorization procedures, both for normal processing and for when the connection with V.I.P. cannot be made or when the processing center is down.
- Chargeback, returned item, and representment procedures.
- Procedures for merchant settlement.

Acquirers must provide any necessary merchant training on procedures and guidelines for handling card transactions established in merchant agreements.

4.2.2 PIN Security

Acquirer centers that process transactions with PINs must provide network security between POS and ATM locations and their own card processing system. Centers must comply with Visa rules for the security of PINs in requests they send to the VIC.

Refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals for system-specific information about PINs and PIN security requirements. Refer to the *Payment Technology Standards Manual* for complete regulations governing PINs.

4.2.3 Response Procedures

Acquirer centers must be able to convert V.I.P. responses into the response messages or the terminal displays needed at the POS or at the ATM. When centers convert responses according to the specifications required by the POS or by the ATM, they must not change the meaning of the issuers' responses.

Acquirer centers must establish procedures to handle non-routine responses from issuers, for instance, BASE I referrals or Interlink partial approvals.

4.2.4 Merchant Central File Management

Acquirer centers wanting to use the Merchant Central File Service (MCFS) must establish the policies and procedures necessary to maintain its entries in the Merchant Central File at the VIC. This file management involves establishing the controls necessary to ensure data accuracy and the procedures for conveying updates to the VIC. Refer to *V.I.P. System Services, Volume 2*, for a description of the Merchant Central File and of MCFS.

4.2.5 Follow-Up Procedures and Processing

Acquirer centers must establish policies on time-out values. They must allow an adequate time for issuer centers to respond but need to be responsive to the time-out demands of their own electronic terminals and ATMs. If the response to a request times out:

- BASE I acquirer centers must send a repeat of the request.
- SMS acquirer centers must reverse the request and send a new request with new key data.

Refer to *V.I.P. System BASE I Technical Specifications* and to the V.I.P. System SMS technical specifications manuals for rules for the use of repeats.

Acquirer centers must support reversal messages.

- BASE I centers use reversals to cancel previously approved transactions.
- SMS centers must use reversals to cancel customer transactions and to handle timed-out requests. They must also be prepared to receive reversal advices from SMS. When an approval response cannot be delivered to an acquirer, SMS generates a reversal advice. In this case, SMS generates a reversal request for the issuer and generates a reversal advice for the acquirer.

Acquirer centers must establish policies and procedures for processing chargebacks and representments, as well as for adjustments for merchandise returns, for failures at ATMs, and for other back office corrections. Acquirer centers must also establish procedures for complying with requests for originals and for copies of sales drafts.

In addition, BASE I acquirer centers must:

- Support Visa and Plus transactions with BASE II batch transaction records if they support these products.
- Generate ATM confirmation messages (*non-U.S. regions only*), as required by the *Visa Operating Regulations*.

SMS acquirer centers also must support chargebacks, representments, adjustments, and copy requests using SMS online messages.

4.2.6 Other Responsibilities

Acquirer centers are also generally responsible for various other tasks external to V.I.P. processing. Examples include:

- Processing merchant deposits after BASE I processing.
- Maintaining merchant accounts.
- Managing acquirer-to-merchant settlement.

For a detailed description of acquirer responsibilities, see *V.I.P. System BASE I Processing Specifications* and the V.I.P. System SMS processing specifications manuals.

4.3 ISSUER PROCESSING CENTER REQUIREMENTS

The following requirements apply to issuer processing centers that want to implement V.I.P. card transaction processing:

- Transaction authorization
- Cardholder Database management
- PIN security
- Coordination with Visa
- Response procedures
- Follow-up procedures and processing
- Other responsibilities

The following subsections explain these requirements.

4.3.1 Transaction Authorization

Issuers must establish policies for making authorization decisions and for keeping cardholder records, including specifications for using V.I.P. stand-in processing (STIP).

An issuer processing center must provide authorization decisions for its cardholders' transactions during normal system processing availability and during downtime. Authorization processing normally involves a computer authorization system with files that provide open-to-buy and account balance totals for each cardholder account.

Accordingly, issuer centers are responsible for maintaining their own records of:

- Cardholders' credit limits.
- Account balances.
- Card restrictions.
- Card statuses, such as:
  - Lost
  - Stolen
  - Fraudulent
  - Pickup

Issuer centers must also maintain the cardholder records kept in the files at the VIC used for STIP functions.

4.3.2 Cardholder Database Management

If an issuer center uses any of the STIP authorization services, it must establish the policies and procedures necessary to maintain its Cardholder Database files at the VIC. Procedures include establishing the controls necessary to ensure the accuracy of cardholder statuses and data plus the methods for conveying updates to the VIC. Refer to *V.I.P. System Services, Volume 2*, for a description of the Automatic Cardholder Database Update (Auto-CDB) Service, which enables issuers to update exception files in response messages.

4.3.3 PIN Security

The issuer processing center is responsible for the method of PIN generation and verification and the rules for PIN usage. Visa issuers can optionally use the PIN Verification Service (PVS) to satisfy this requirement. Refer to *V.I.P. System Services, Volume 2*, for a description of PVS.

Refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals for system-specific information about PINs and PIN security

requirements. Refer to the *Payment Technology Standards Manual* for complete regulations governing PINs.

4.3.4 Coordination With Visa

The issuer center or the issuer itself must provide Visa with all of the processing parameters that the V.I.P. System is to use for the issuer's cardholders. These parameters include those that determine:

- Routing of requests.
- Verification of PINs and Card Verification Values (CVVs and iCVVs) at the VIC.
- STIP authorization decisions.

Issuer centers must establish procedures for notifying Visa, well in advance, whenever any processing requirements or parameters change.

4.3.5 Response Procedures

Issuer centers must be able to respond to requests within a reasonable time frame. Regions establish Automated Response Time (ATR) time limits. The limits vary by region and by card program.

If the issuer does not respond to a request or to a reversal within the established ATR limit, V.I.P. routes the request or the reversal to STIP. Upon receiving the request, STIP then provides the authorization decision on behalf of the issuer center. If an SMS issuer does not respond to an SMS acquirer-generated advice within the ATR limit, STIP responds for the issuer center and stores the advice for later recovery.

4.3.6 Follow-Up Procedures and Processing

Issuer centers must be able to receive and to appropriately process repeats, second submissions, or both, of the same customer transaction. They must also receive and process reversals.

SMS issuer centers must also provide the following, depending on the card products they choose to process:

- Support for transaction and reversal advices. Advices can be generated by STIP, by SMS, and by BASE II.
- Support for adjustments and for merchandise returns.
- Chargeback procedures and support for chargeback messages.
- Support for representments.
- Other program-unique functions, such as the downtime resubmissions of Interlink transactions.

BASE I issuer centers handle such functions through BASE II or through similar outside systems.

SMS issuer centers need a high level of transaction control to ensure that all of the messages related to any one customer transaction are properly tracked and processed. While SMS checks transaction consistency, issuer centers have ultimate responsibility for validating incoming messages. For instance, if a merchandise return occurs several days after the original purchase, SMS cannot check the adjustment message against the original request. This kind of checking must be implemented by the issuer center.

Issuer centers must have procedures in place for responding to cardholder requests for copies or for originals of disputed sales drafts.

- BASE I centers must handle these requests through BASE II or through similar outside systems.
- SMS centers must support SMS copy request messages and their confirmations.

4.3.7 Other Responsibilities

In addition, issuer processing centers are also responsible for:

- The rules and the fees for card usage.
- The method of CVV or iCVV verification, if any, for Visa transactions. Visa issuers can optionally use the Card Verification Value (CVV) Service to satisfy this requirement. Refer to *V.I.P. System Services, Volume 2*, for a description of the CVV Service.
- Posting to cardholder accounts and preparing cardholder invoices.
- Lost or stolen card reporting and other fraud control methods.
- Determining their policy for address verification of mail and telephone order and airline transactions. Issuers can optionally use the Address Verification Service (AVS) to satisfy this requirement. Refer to *V.I.P. System Services, Volume 2*, for a description of the AVS Service.

Issuer centers may also be responsible for other tasks at the request of the issuer, such as issuing cards, with PIN Verification Values (PVVs) and CVVs or iCVVs, as applicable, issuing PINs, or posting transactions settled through BASE II.

Appendix A

Transaction Types

Most transactions are initiated by cardholders at an ATM or at the point of sale; other transactions are initiated by merchants, by acquirers, or by issuers. Some transactions are system-generated; others are initiated during issuer or acquirer back office processing.

Table A-1 lists V.I.P. financial transactions. A check mark in the BASE I or the SMS column indicates that the transaction type is available for processing under BASE I, under SMS, or under both. The following section further describes V.I.P. transactions.

Table A-1 V.I.P. Transaction Types

Transaction Type	BASE I	SMS
Cardholder Transactions		
Authorization or Verification Request	✓	✓
ATM Cash Disbursement	✓	✓
Manual Cash Disbursement	✓	✓
Purchase	✓	✓
• Purchase With Cashback	✓	✓
• Quasi-Cash	✓	✓
• Key-Entered Purchase	✓	✓
• Scrip		✓
• Purchase With Address Verification	✓	✓
Deferred Clearing Purchase	✓	✓
Below Floor Limit Purchase		✓
Preauthorization		✓
Merchandise Return		✓
Balance Inquiry	✓	✓
Address Verification Only	✓	✓
Merchant-Authorized Transactions		
Store-and-Forward		✓
Paper Sales Draft (Online Financial)		✓
Resubmission		✓
System-Generated Transactions		
Reversal	✓	✓
Cash Disbursement Adjustment		✓

Table A-1 V.I.P. Transaction Types (continued)

Transaction Type	BASE I	SMS
Exception Transactions		
Adjustment		✓
Good Faith Collection		✓
Chargeback		✓
Chargeback Reversal		✓
Representment		✓
Fee-Related Transactions		
Acquirer-Initiated Fee Collection/Funds Disbursement		✓
Issuer-Initiated Fee Collection/Funds Disbursement		✓
Reconciliation Transactions		
Reconciliation Request/Response		✓
File Maintenance Transactions		
File Update or Inquiry Request	✓	✓
Administrative Transactions		
Card Capture Notification	✓	✓
Free Text Message	✓	✓
Copy Request/Confirmation		✓
Online Fraud Reporting		✓
Network Management Transactions		
Network Management Request/Response	✓	✓

A.1 CARDHOLDER TRANSACTIONS

The following section describes the types of cardholder transactions.

Authorization or Verification Request—Acquirers use this transaction to request authorization of a transaction or to verify account or address information.

ATM Cash Disbursement—This transaction is used for cash disbursements from automated teller machines (ATMs).

Manual Cash Disbursement—A manual cash disbursement (also called manual cash) is a transaction with which the cardholder obtains cash in a face-to-face environment. It is available for Visa POS and for Visa Electron.

Cardholder Transactions

Purchase—This transaction type includes the basic purchase transaction as well as the following variations:

- Purchase With Cashback—This transaction is a variation of the purchase transaction that permits the cardholder to obtain cash in addition to goods or services.
- Quasi-Cash—This transaction 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 POS and for Visa Electron.
- Key-Entered Purchase—This transaction is a variation of the purchase transaction, used only for Visa POS transactions as allowed by *Visa Operating Regulations* when the magnetic stripe on the card is not readable.
- Scrip (Interlink only)—Scrip is a paper receipt that can be exchanged by the bearer for goods or services combined with cash, as specified by the merchant. These transactions are used by United States (U.S.) merchants with self-service terminals that dispense scrip. Scrip transactions are available only for Interlink acquirers in the U.S. region. Scrip transactions must be supported by Interlink issuers outside of the U.S. region for the convenience of their cardholders when they are in the U.S. region, but they are not offered to acquirers outside the United States.
- Purchase With Address Verification—This transaction is used by Visa merchants such as direct marketing firms and airlines to verify a cardholder's address as part of a purchase request.

Deferred Clearing Purchase—This transaction is used by merchants such as hotels and car rental agencies when the purchase amount is not known at the time a transaction is authorized. This transaction may be preceded by an authorization request. The message used to convey deferred clearing information is a *deferred clearing advice*.

Below-Floor-Limit Purchase—This transaction is used by Visa merchants when the transaction amount is below the floor limit. Because below-floor-limit transactions need not be authorized, this transaction cannot be declined. This transaction is available only for Visa POS. It is not available for Visa Electron.

Preauthorization (Interlink only)—A preauthorization is designed for merchant locations such as gas stations where the purchase amount is not known at the time the transaction is initiated. Preauthorizations consist of an initial request message followed by a completion message. The transaction must be completed within two hours. The merchant is guaranteed payment if:

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

Merchandise Return—A merchandise return transaction permits a merchant to credit the account of a cardholder who returns merchandise for the entire or partial amount.

Balance Inquiry—A balance inquiry allows a cardholder to check his or her account balance at an ATM, at a stand-alone merchant terminal away from the point of sale, and at the point of sale or point of service.

Address Verification Only—This transaction is used by Visa merchants such as direct marketing firms and airlines to verify a cardholder's address before submitting a purchase transaction.

A.2 MERCHANT-AUTHORIZED TRANSACTIONS

Store-and-forward transactions and Interlink-only paper sales draft transactions are used by merchants by prior arrangement with the acquirer when the merchant systems are down or are unable to communicate with the acquirer. These transactions must be processed within nine (9) calendar days following the date of the original transaction. Neither the issuer nor Visa is liable for any losses resulting from merchant-authorized transactions, nor is the merchant guaranteed payment for them.

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

NOTE

Merchandise credits are not allowed for the POS Check Service.

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

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

EXAMPLE

For instance, a merchant may choose to complete a declined transaction for a regular customer, even though the issuer declined the transaction because of daily limits, with the expectation that the transaction will be approved when the merchant resubmits it the next day.

Acquirers can resubmit transactions once a day for nine (9) calendar days following the date of the cardholder's transaction (not the date of the denial). After nine days, V.I.P. rejects further resubmission attempts.

A.3 SYSTEM-GENERATED TRANSACTIONS

There are two types of system-generated transactions:

Reversal—A reversal transaction is used to reverse an approved authorization, a preauthorization, or a financial transaction that was not completed due to a system malfunction or because the transaction timed out. Financial transactions are cash disbursements, purchases (all variations), merchandise credits, POS cancellations, store-and-forward transactions, paper sales draft transactions, and resubmissions. (Deferred clearing purchases and below-floor-limit purchases cannot be reversed.) A reversal transaction can be initiated by an ATM, by an acquirer's host system, or by V.I.P. In contrast to an Interlink POS cancellation,

which is initiated by the cardholder or by merchant personnel, a reversal transaction is system-generated.

Cash Disbursement Adjustment—This transaction is a system-generated adjustment (debit or credit) used by an ATM acquirer to adjust the value of a cash disbursement because of an ATM misdispense or a late completion.

A.4 EXCEPTION TRANSACTIONS

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

Adjustment—An acquirer creates an adjustment to an original transaction to correct an error such as an out-of-balance condition at the point of sale. The adjustment may be either a debit or a credit.

Good Faith Collection (Interlink only)—An Interlink acquirer may use this variation of the adjustment if the issuer agrees to accept a financial transaction that cannot be processed under Interlink rules, typically because time frames for exception processing have expired.

Chargeback—An issuer creates a chargeback when a cardholder disputes a transaction, when a cardholder asserts that merchandise was returned but a merchandise credit has not been received by the issuer, when the issuer itself disputes a transaction, or when the issuer receives an unpostable debit adjustment from an acquirer.

Chargeback Reversal—An issuer creates a chargeback reversal to cancel a prior chargeback that was sent in error. This transaction is not used in the Interlink Service.

Representment—An acquirer creates a representment when the validity of a chargeback can be disproved.

A.5 FEE-RELATED TRANSACTIONS

Fee-related transactions do not require authorization and may not be declined. These transactions are not used in the Interlink or the Plus service. There are two types of fee-related transactions:

Fee Collection—This transaction is used to collect miscellaneous fees.

Funds Disbursement—This transaction is used to remit miscellaneous fees.

A.6 RECONCILIATION TRANSACTIONS

Members may use the optional reconciliation transaction to receive batch financial totals of transactions at half-hour intervals and at the end of the day. SMS participants use these reconciliation totals to verify processing totals. Participants can also initiate an online message at any time to receive the previous day's end-of-day totals or to receive current reconciliation totals as of the last half-hour batch cutoff.

A.7 FILE MAINTENANCE TRANSACTIONS

File maintenance transactions are used by issuers to update or to query Cardholder Database files such as the Exception File, the Address Verification File, or the PIN Verification File. See the "Managing System Databases" section of Chapter 2, V.I.P. Transaction Processing, for more information on the Cardholder Database files.

A.8 ADMINISTRATIVE TRANSACTIONS

Administrative messages, which are initiated by a participant's operations staff, are used to request or to convey information between the issuer and the acquirer. There are four types of administrative messages:

Card Capture Notification—This transaction is used by a Plus acquirer to notify a Plus issuer that a card has been captured when one of the participants is connected to Plus System, Inc.

Free-Text Message—This transaction is used to provide or to request information of a general nature for transactions.

Copy Request/Confirmation—Copy requests and copy confirmations are used to process requests fro documentation. These transactions are not used for ATM or Interlink transactions.

Online Fraud Reporting—These transactions are used by members to report, track, and analyze fraudulent transactions.

A.9 NETWORK MANAGEMENT TRANSACTIONS

Network management transactions are used to perform the following functions:

Sign-On—The sign-on transaction is used by issuers and by acquirers to notify VisaNet that they are available to send and to receive messages.

Sign-Off—The sign-off transaction is used by issuers and by acquirers to notify VisaNet that they are not available.

Recovery Sign-On—This transaction is used by issuers and by acquirers to request delivery of advice messages by signing on to Advice Recovery mode.

Recovery Sign-Off—This transaction is used by issuers and by acquirers to indicate that they do not want to receive further advice messages and are signing off from Advice Recovery mode.

Reconciliation Request—This request is used optionally by issuers and by acquirers to request current processing totals.

Echo Test—An echo test is used by issuers, by acquirers, and by V.I.P. to confirm the availability of the communications link between the member host system and VisaNet.

Dynamic Key Exchange—This transaction is used optionally by issuers, by acquirers, and by V.I.P. to update working keys online.

For additional information on V.I.P. transactions, refer to *V.I.P. System BASE I Processing Specifications* and to the V.I.P. System SMS processing specifications manuals.

Index

A

Account Verification Service 3-10
acquirer responsibilities
establishing follow-up procedures 4-5
establishing Merchant Central File policies 4-5
establishing POS connection 4-3
establishing response procedures 4-4
processing options, Card Recovery Bulletins 3-6
providing PIN security 4-4
Address Verification Service (AVS) 3-10
administrative
messages 2-9
Advice File
BASE I 3-11
SMS 3-11
advice recovery 2-7, 2-9, 4-2
ATM cash disbursement A-2
ATM Format Conversion Service 3-11
ATM Transaction Processing Integration 3-16
ATM/POS Split Routing Service 3-4
ATR (Assured Transaction Response) 2-9
authorization
definition of 1-1
issuer responsibilities 4-6
request A-2
services
Account Verification Service 3-10
Address Verification Service (AVS) 3-10
ATM Format Conversion Service 3-11
availability 3-15
BASE I Advice Retrieval Service 3-11
Card Verification Value (CVV) Service 3-11
Card Verification Value 2 (CVV2) Service 3-11
Cardholder Authentication Verification Value (CAVV) Verification Service 3-12
Custom Payment Service (CPS)/ATM 3-12
Custom Payment Service (CPS)/POS 3-12
Deferred Clearing Advice File (DCAF) Service 3-12
Dynamic Key Exchange (DKE) Service 3-13
Full Authorization Service 3-13
International Automated Referral Service (IARS) 3-13
Multicurrency Service 3-13
PIN Verification Service (PVS) 3-13
POS Check Service 3-13
Positive Authorization Capacity Management (PACM) Service 2-6, 3-13
Positive Cardholder Authorization Service (PCAS) 2-6, 3-14
SMS Advice Retrieval Service 3-11
Status Check Service 3-14
VisaPhone Service 3-15
authorization database services
Automatic Cardholder Database Update (Auto-CDB) Service 3-9
availability 3-10
Merchant Central File Service (MCFS) 3-9
Automatic Cardholder Database Update (Auto-CDB) Service 3-9
AVS. See Address Verification Service 3-10

B

balance inquiry A-3
BASE I Advice Retrieval Service 3-11
BASE I System
description of 1-6
reports 2-12

stand-in processing (STIP) 2-6 to 2-8
BASE II System 1-8
billing 2-13

C

Card Recovery Bulletin (CRB) Service 3-6
Card Verification Value (CVV) Service 3-11
Card Verification Value 2 (CVV2) Service 3-11
Cardholder Authentication Verification Value (CAVV) Verification Service 3-12
Cardholder Database
Advice File—BASE I 3-11
Advice File—SMS 3-11
description of 2-10
issuer responsibilities 4-6
cardholder transactions A-2
CAVV. See Cardholder Authentication Verification Value (CAVV) Verification Service 3-12
certification 4-2
Chargeback Reduction Service (CRS) 3-16
Check Acceptance Service 3-4
chip card services
availability 3-9
Visa Cash Service 3-8
Visa Horizon Service 3-8
clearing
definition of 1-12
clearing, definition of 1-1
Common Member Interface (CMI)
overview 1-10
processes 1-10
CPS. See Custom Payment Service 3-12
CRS. See Chargeback Reduction Service 3-16
Custom Payment Service (CPS)/ATM 3-12
Custom Payment Service (CPS)/POS 3-12
CVV (Card Verification Value)
in STIP 2-8
result code processing 2-8
CVV. See Card Verification Value (CVV) Service 3-11
CVV2. See Card Verification Value 2 (CVV2) Service 3-11

D

DCAF. See Deferred Clearing Advice File Service 3-12
deferred clearing
definition of 1-2
purchase A-3
Deferred Clearing Advice File (DCAF) Service 3-12
deposit access products
comparison of 1-3
Plus 1-3
Visa Cash 1-2
Visa Debit 1-2
Visa Electron 1-2
Visa Horizon 1-2
Visa Interlink 1-3
dual-message transaction, definition of 1-2
Dynamic Key Exchange (DKE) Service 3-13

E

establishing POS connection 4-3
Exception File
automatic updating 2-11
description of 2-11

F

fee-related transactions
A-5
file
maintenance transactions
A-5
files
Advice File—BASE I 3-11
Advice File—SMS 3-11
financial transactions, types of A-1
Fraud Reporting System (FRS) 3-7
Full Authorization Service 2-11, 3-13

G

Gateway Services 3-4

I

Integrated Debit Service 3-5
International Automated Referral Service (IARS) 3-13
issuer processing options, Card Recovery Bulletins 3-6
issuer responsibilities
establishing authorization policies 4-6

establishing Cardholder Database file policies 4-6
establishing follow-up procedures 4-7
establishing response procedures 4-7
managing processing parameters 4-7
providing PIN security 4-6

L

linking related messages 2-4
logging, VisaNet Integrated Payment (V.I.P.) System 2-9

M

manual cash disbursement A-2
matching messages 2-4
MCFS. See Merchant Central File Service 3-9
Merchant Central File
acquirer responsibilities 4-5
description of 2-12
Merchant Central File Service (MCFS) 3-9
merchant-authorized transactions
paper sales draft A-4
resubmission A-4
store-and-forward A-4
message
bit map 2-4
data fields 2-4
editing 2-2
formats 1-13, 2-2
header 2-4
response processing 2-8, 4-4, 4-7
sets 2-4
support 4-1
type identifier 2-4
V.I.P. structure 2-3
message flows
normal processing
administrative transactions A-6
file maintenance transactions A-5
merchant-authorized transactions A-4
network management transactions A-6
reconciliation transactions A-5
system-generated transactions A-4
Multicurrency Service 3-13

N

network management 2-9, 4-2
network stations 4-1
normal processing
administrative transactions A-6
file maintenance transactions A-5
merchant-authorized transactions A-4
network management transactions A-6
system-generated transactions A-4

O

online deferred clearing, definition of 1-2

P

PACM. See Positive Authorization Capacity Management Service 3-13
paper sales draft
transaction A-4
parameters
issuer managing 4-7
stand-in processing (STIP) 2-6
V.I.P. 1-12
PCAS. See Positive Cardholder Authorization Service 3-14
PIN security 4-4, 4-6
PIN Verification Service 2-11
PIN Verification Service (PVS) 3-13
PIN/No-PIN Split Routing Service 3-5
POS Check Service 3-13
POS connection, setting up 4-3
Positive Authorization Capacity Management (PACM) Service 3-13
Positive Cardholder Authorization Service (PCAS) 3-14
Preauthorization A-3
Priority Routing Service 3-5
processing
BASE I 1-6
BASE II 1-8
Common Member Interface (CMI) 1-10
networks 1-1
parameters
issuer responsibilities 4-7
stand-in processing (STIP) 2-6
V.I.P. 1-12
Single Message System (SMS) 1-7

processing center
certification 4-2
description of 1-4
establishing 4-1
network management 4-2
requirements
acquirer 4-3, 4-5
issuer 4-6, 4-8
testing 4-2
processing flow, transaction 2-1
purchase
below-floor-limit A-3
key-entered A-3
with address verification A-3
with cashback A-3

Q

quasi-cash A-3

R

raw data records 2-13
reports
BASE I 2-12
resubmission transaction A-4
reversal
transaction
system-generated A-4
risk management services
availability 3-7
Card Recovery Bulletin (CRB) Service 3-6
Fraud Reporting System (FRS) 3-7
routing
alternatives 2-6
defined 2-4
information
stand-in processing (STIP) 2-6
system tables 2-5
internal 2-6
services
ATM/POS Split Routing Service 3-4
availability 3-6
Check Acceptance Service 3-4
Gateway Services 3-4
Integrated Debit Service 3-5
PIN/No-PIN Split Routing Service 3-5
Priority Routing Service 3-5
Visa Shortest Online Path Service (VSOP) 3-5
tables 2-5

S

Scrip A-3
services
VisaNet Settlement Service (VSS) 1-11
settlement
definition of 1-12
settlement entity, definition of 4-3
settlement, definition of 1-1
SI mode 2-9, 4-2
sign on / sign off 2-9, 4-2
Single Message System (SMS)
description of 1-7
overview 1-7
reconciliation requirements 4-2
stand-in processing (STIP) 2-8
single message transaction, definition of 1-2
SMS Advice Retrieval Service 3-11
SMS. See Single Message System 1-7
stand-in processing
through V.I.P. (STIP)
BASE I 2-6
stand-in processing (STIP)
through V.I.P.
BASE I 2-7 to 2-8
parameters 2-6
Single Message System (SMS) 2-8
Status Check Service 3-14
STIP. See stand-in processing 2-6
store-and-forward
transaction A-4
system databases
Cardholder Database files 2-10
managing 2-10
Merchant Central File 2-10
system globals. See system tables 2-9

system parameters. See processing, parameters 2-6
system tables 2-9
routing 2-5
system-generated transaction
reversal A-4

T

test messages 2-9, 4-2
testing 4-2
transaction flow 2-1
transaction processing
authorization 1-1
clearing 1-1
dual message 1-2
illustration of flow 2-1
illustration of systems 1-5
online deferred clearing 1-2
settlement 1-1
single message 1-2
transaction tracing 2-4
transaction types
cardholder A-2
fee-related
A-5
list of A-1
transactions
file maintenance
A-5
paper sales draft A-4
resubmission A-4
reversal
system-generated A-4
store-and-forward A-4

V

VAP. See VisaNet Access Point 1-4
VIC. See VisaNet Interchange Center 1-4
Visa Cash Service 3-8
Visa check card II 3-16
Visa Horizon Service 3-8
Visa Issuer Fraud Detection (VIFD) Service
VIFD 3-1
Visa Secure Electronic Commerce (VSEC) services
availability 3-8
Visa Shortest Online Path Service (VSOP) 3-5
Visa Smart Debit/Smart Credit (VSDC) Service 3-8
Visa/Plus ATM Transaction Processing Integration 3-16
VisaNet
BASE II System 1-8
components 1-1, 1-3
systems 1-5
transaction processing 1-5
V.I.P. processing parameters 1-12
VisaNet Access Point (VAP)
description of 1-4
network stations 4-1
VisaNet Integrated Payment (V.I.P.) System
backup 1-5
billing 2-13
components
BASE I System 1-6
Common Member Interface (CMI) 1-10
Single Message System (SMS) 1-7
logging 2-9
overview 1-6
processing
parameters 1-12
reports 2-12
services, listed by functional group 3-1
VisaNet Interchange Center (VIC), description of 1-4
VisaNet Settlement Service (VSS)
considerations 4-3
definition 1-11
reports 2-12
VisaPhone Service 2-11, 3-15
VSEC. See Visa Secure Electronic Commerce 3-7
VSOP. See Visa Shortest Online Path Service 3-5