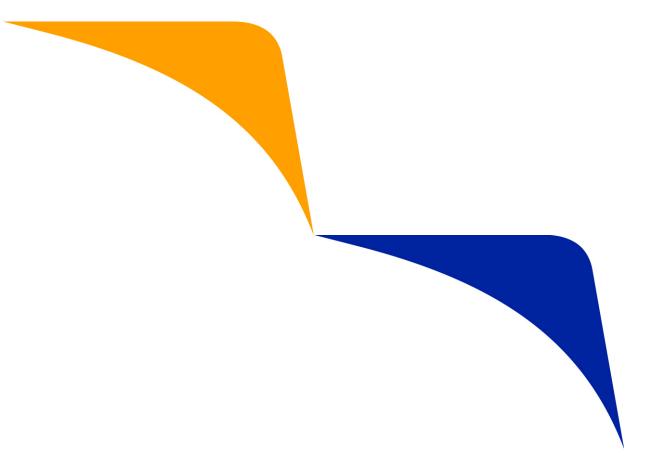


Verified by Visa

Acquirer and Merchant Implementation Guide U.S. Region

May 2011





Verified by Visa Acquirer and Merchant Implementation Guide

U.S. Region

May 2011

DISCLAIMER: THE RECOMMENDATIONS CONTAINED HEREIN ARE INTENDED FOR INFORMATIONAL PURPOSES ONLY AND SHOULD NOT BE RELIED UPON FOR MARKETING, LEGAL, TECHNICAL, TAX, FINANCIAL OR OTHER ADVICE. WHEN IMPLEMENTING ANY NEW STRATEGY OR PRACTICE, YOU SHOULD CONSULT WITH YOUR LEGAL COUNSEL TO DETERMINE WHAT LAWS AND REGULATIONS MAY APPLY TO YOUR SPECIFIC CIRCUMSTANCES. THE ACTUAL COSTS, SAVINGS AND BENEFITS OF THE VERIFIED BY VISA SERVICE MAY VARY BASED UPON YOUR SPECIFIC BUSINESS NEEDS AND PROGRAM REQUIREMENTS. PLEASE NOTE THAT THAT VISA MAKES NO REPRESENTATIONS AND WARRANTIES AS TO THE INFORMATION CONTAINED HEREIN AND MEMBER IS SOLELY RESPONSIBLE FOR ANY USE OF THE INFORMATION IN THIS PRESENTATION IN CONNECTION WITH ITS CARD PROGRAMS.

THIS DOCUMENT IS PROVIDED ON AN "AS IS", "WHERE IS" BASIS, "WITH ALL FAULTS" KNOWN AND UNKNOWN. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VISA EXPLICITLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE INFORMATION IN THIS DOCUMENT, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. YOU ARE SOLELY RESPONSIBLE FOR YOUR USE OF THE INFORMATION CONTAINED HEREIN.

Contents

A	About This Guide 1		
1	v	erified by Visa Overview	7
	1.1	Technology Platform	7
	1.2	Channels and Technologies Supported	7
	1.3	Verified by Visa Overview	8
	1.4	Authorization versus Authentication	8
	1.5	Summary of Verified by Visa Benefits	9
	1.6	Merchant Benefits	10
	1.7	Merchant Marketing Opportunities	12
2	3	-D Secure Technology Platform	13
	2.1	3-D Secure Participants	14
	2.2	Software Components	15
3	т	ransaction Flows	17
	3.1	Cardholder Enrollment/Activation	17
	3.2	Online Purchases	18
4	3	-D Secure Messages	23
	4.1	Verify Enrollment Messages	23
	4.2	Payer Authentication Messages	25
	4.3	Handling of the Merchant Password Field in 3-D Secure Messages	27
	4.4	Attempted Authentication Exclusions	27
	4.5	Merchant Type Exclusions	28
	4.6	Cache Messages	28
5	Α	uthorization Processing	29
	5.1	Electronic Commerce Indicator (ECI)	30
	5.2	Cardholder Authentication Verification Value and Authentication Identifier	31
	5.3	Authentication and Authorization	32
	5.4	PARes Fields for Authorization Requests	35
	5.5	Electronic Commerce Custom Payment Service Qualification	36
	5.6	ACI and ECI Values Must Be Consistent	37
	5.7	No Re-Use of Authentication Data	37

	5.8 Recurring Transactions	38
	5.9 Installment Transactions	39
	5.10 Online Auctions	39
	5.11 Authentication Data Limits	39
6	Merchant Server Plug-In Functions	40
	6.1 Message Processing Functions	40
	6.2 Additional MPI Functional Requirements	41
7	Acquirer/Merchant Requirements and Best Practices	44
	7.1 Acquirer Responsibility for Merchant Participation	44
	7.2 Merchant Authentication to Access Visa Directory Server	45
	7.3 Pre-Authentication Messaging at Checkout	45
	7.4 Use of Framed Inline Page	47
	7.5 Text for Inline Page with a Framed Window	48
	7.6 Use of Verified by Visa Merchant Symbol	49
	7.7 Activation Anytime	50
	7.8 Failed Authentication Processing	50
	7.9 Merchant Performance Standards	51
	7.10 Data Quality in VEReq and PAReq Messages	51
	7.11 Timing between VERes and PAReq	53
	7.12 Merchant Customer Support	53
8	Digital Certificate Use	54
	8.1 Visa Certificate Hierarchy	54
	8.2 Merchant Authentication	55
	8.3 Transport Security	56
9	MPI Implementation Options	57
	9.1 Buy Options for MPI Software	58
	9.2 Hosted MPI Options	59
	9.3 Custom Software Development	60
1(0 Implementation Considerations	61
	10.1 Participation, Decision, and Project Team	61
	10.2 Development Phase	62
	10.3 Testing Phase	63
	10.4 Requirements for Pre-Production Readiness via Product Integration Testing (PIT)	64

1	0.5	Pre-Production Implementation Checklist	66
1	0.6	Merchant MPI System Resiliency	66
11	Ri	sk Management	69
1	1.1	Related Security Programs	70
1	1.2	Excessive Chargebacks and/or Fraud	70
1	1.3	Visa Cardholder Information Security Program (CISP)	71
1	1.4	Verified by Visa Global Performance Standards	71
12	Di	spute Resolution	72
1	2.1	Applicable Operating Regulations	72
1	2.2	Merchant Transaction Records	73
1	2.3	Dispute Processing – Acquirer Quick Reference	74
13	Fo	r Acquirers	76
1	3.1	Acquirer Role in Verified by Visa	76
1	3.2	Visa Directory Server: Acquirer and Merchant Registration	78
1	3.3	Acquirer Processing Requirements	78
1	3.4	Sample Acquirer Project Plan	80
A	١р	pendices	
Α	Pla	anning and Implementation Example for Merchant Plug-In	83
в	Ve	rified by Visa Activation Anytime	90
С	Be	st Practices for Fraud Screening	93
D	Vb	V Global Performance Enhancement Program	96
Glo	ssa	ry	99
Ind	ex		105

Tables

Table 1:	Document Conventions	4
Table 2–1:	Roles of Verified by Visa Program Participants	14
Table 4–1:	Verify Enrollment Messages	23
Table 4–2:	Verify Enrollment Response Values	23
Table 4–3:	Payer Authentication Messages	25
Table 4–4:	Issuer Authentication Results Values	26
Table 5–1:	Transaction Status Values	29
Table 5–2:	3-D Secure Response Mapping Exhibit	33
Table 5–3:	PARes Fields Required for Authorization Messages	35
Table 5–4:	ACI and ECI Values for Authorization Messages	37
Table 7-1:	Payer Authentication Request Message Fields	52
Table 8-1:	Visa Certificate Hierarchy	54
Table 10-1:	Required Merchant Implementation Checklist	66
Table 12-1:	Dispute Processing Summary Acquirers – Authenticated Trans	74
Table 12-2:	Dispute Processing Summary Acquirers – Attempted Authentications	75
Table 13–1:	Sample Acquirer Project Plan	80
Table A–1:	Example Planning and Implementation Checklist	88
Table A–1:	Example Planning and Implementation Checklist (Continued)	89
Table D-1.	VbV Global Performance Program Standards	97

Figures

Figure 2-1: The Three Domains of 3-D Secure	15
Figure 3–1: Purchase Transaction Flow	19
Figure 3–2: Verified by Visa Password Entry Screen	21
Figure 5–1: Determining Whether to Submit Authorization	32
Figure 7-1: Merchant Checkout Page with Pre-Authentication Messaging	46
Figure 7-2: Inline Page with Top Frame	47
Figure 7–3: Inline Page with Side Frame	48
Figure B-1: Activation Anytime Landing Page	90
Figure B-2: Sample Issuer Activation Page	91
Figure B-3: Sample Password Creation Page	91
Figure B-4: Sample Activation Successful Page	92

About This Guide

The requirements in this publication are referenced in the *Visa International Operating Regulations*, and have the same authority as the *Visa International Operating Regulations*. They are binding upon participants in the services referenced. The *Visa International Operating Regulations* govern in the event of any inconsistency or contradiction, unless Visa specifically grants a variance.

Acquirers and merchants are required to adhere to the requirements set forth in this Guide and any related addendums to this Guide. Any differences in implementation **must** be approved in writing by Visa prior to production launch. Ask your Visa Representative for information.

Trademarks

Visa®, Verified by Visa® and 3-D Secure® are registered trademarks or trademarks of Visa Inc. in the United States and other countries.

Purpose

This document is intended to assist acquirers, merchants, and merchant processors in their implementation of Verified by Visa (VbV), by helping them to:

- Understand the functionality, uses, and benefits of the Verified by Visa program.
- Plan the development, testing, certification, and production setup of the Verified by Visa program.

Audience

The Verified by Visa Acquirer and Merchant Implementation Guide is intended for acquirers, merchants, and processors that are evaluating or have decided to implement Verified by Visa. This guide explains the Verified by Visa program and its benefits, transaction flows, and implementation planning considerations.

Changes from Prior Publication

This publication was updated from the prior version as shown below.

New Content	Where to Find the Content in This Guide
A new section was added with System Resiliency recommendations.	Chapter 10, Implementation Considerations: Section 10.6, Merchant MPI System Resiliency

Organization of This Guide

This document contains the following sections:

About This Guide – This introductory section highlights the topics covered in the Guide as well as the conventions used throughout the Guide, and provides a list of Verified by Visa resources and tools.

- 1. **Verified by Visa Overview**—This chapter provides a high-level summary of Verified by Visa and the benefits of acquirer and merchant participation.
- 2. **3-D Secure Technology Platform**—This chapter describes the roles of participants in the Verified by Visa program and the key software components used by each.
- 3. **Transaction Flows**—This chapter describes cardholder enrollment/activation and purchase authentication transaction flows.
- 4. **3-D Secure Messages**—This chapter briefly describes each 3-D Secure message involving acquirers and merchants.
- Authorization Processing—This chapter describes how the MPI determines whether authentication was successful as well as the Electronic Commerce Indicator (ECI), the Cardholder Authentication Verification Value (CAVV), and special processing situations.
- 6. **Merchant Server Plug-In Functions**—This chapter provides an overview of MPI functions, including message processing and other functional requirements.
- Acquirer/Merchant Requirements and Best Practices—This chapter reviews the acquirer and merchant business requirements for Verified by Visa implementations, including cardholder interfaces and performance standards.
- 8. **Digital Certificate Use**—This chapter discusses Verified by Visa use of the Visa-issued certificates, the process of authenticating Verified by Visa merchants to the Visa Directory Server, and the requirements for securing 3-D Secure channels that include the merchant.

- MPI Implementation Options—This chapter reviews some alternatives for implementing Merchant Server Plug-in (MPI) functionality to enable merchant participation in Verified by Visa.
- 10. **Implementation Considerations**—This chapter discusses implementation, ranging from the decision to participate in Verified by Visa through installation, testing, and production integration.
- 11. **Risk Management**—This chapter provides a high-level discussion of electronic commerce risk management functions and related security programs.
- 12. **Dispute Resolution**—This chapter discusses dispute resolution requirements for Verified by Visa transactions.
- 13. For Acquirers—This chapter describes acquirer functions and requirements.

Appendix A. Planning and Implementation Example—This appendix provides an example of planning and implementation steps for merchants that purchase a Merchant Server Plug-in to integrate with the web storefront software at their location.

Appendix B. Verified by Visa Activation Anytime—This appendix provides a description of the Activation Anytime capability that merchants may implement.

Appendix C. Best Practices: Fraud Screening—This appendix provides best practices for reducing the risk of successful fraudulent card activity by identifying fraudulent behavior and risk indicators.

Appendix D. Verified by Visa Global Performance Enhancement Program—This appendix lists the Verified by Visa global performance standards.

Glossary—Defines selected terms related to the Verified by Visa program.

Index—Provides a list of key topics with page number references.

Document Conventions

The document conventions used in this guide are shown in Table 1.

Table 1: D	Ocument Conventions
------------	---------------------

Document Convention	Purpose In This Guide
Boldface	Highlights section title and sub-titles; also the words must or must not are highlighted to call attention to important requirements.
Italics	Document titles; emphasis.
Important	Highlights important information in the text.
Note:	Provides more information about the preceding topic.

Resources and Tools

Documentation has been developed for acquirers and merchants to assist in understanding the 3-D Secure technology platform as well as Verified by Visa program information. These support materials are listed below.

Verified by Visa Publications and Materials

The following are available to Visa acquirers and merchants to assist in Verified by Visa program development. These materials are available through Visa Online at: www.us.visaonline.com

- Verified by Visa Service Description
- Verified by Visa Acquirer and Merchant Implementation Guide
 - 3-D Secure Merchant Client Authentication Digital Certificate Requests, Rules/Instructions and Forms, Addendum to the Verified by Visa Acquirer and Merchant Implementation Guide
- Verified by Visa Issuer Implementation Guide
- Verified by Visa Quick Reference Guide for Merchant Customer Service Representatives
- Verified by Visa Operations and Dispute Resolution Guide
- Verified by Visa artwork, reproduction and application guidelines are available at Visa Online or at <u>www.productbrandstandards.com</u>, Section 3.8, *Verified by Visa*.

Acquirer Materials

• U.S. Interchange Reimbursement Fee Rate Qualification Guide – Acquirers can obtain information about IRF qualification. The Guide is accessible by acquirers through Visa Online.

Merchant Materials

 Visa.com Website – Acquirers and merchants can obtain information about Verified by Visa and the technology that supports Verified by Visa functionality at:

http://usa.visa.com/merchants/risk_management/vbv.html

• *Verified by Visa Merchant Toolkit* provides the Verified by Visa Merchant Symbol graphic and usage standards. Merchants can obtain the Toolkit at:

http://usa.visa.com/merchants/risk management/vbv.html

• The 3-D Secure Technology Provider list is available electronically at:

www.visa.com/3-dsecure

Merchant Risk Management Information

The following are available electronically to Visa acquirers and merchants to provide guidance in assuring that risk management requirements are met:

Cardholder Information Security Program

The Visa Cardholder Information Security Program or CISP is the Visa implementation of the industry standard called the Payment Card Industry (PCI) Data Security Standard (DSS). Supporting PCI DSS, the Visa CISP defines requirements for parties that handle payment card transactions, including merchants, to protect cardholder and transaction information. More information about CISP is available at:

http://usa.visa.com/merchants/risk_management/cisp.html

Electronic Commerce Risk Management Best Practices

Electronic Commerce Risk Management Merchant Best Practices defines business risks and proposed solutions for merchants conducting secure commerce. This document is available at:

http://usa.visa.com/download/merchants/visa risk management guide ecommerce.pdf

3-D Secure Specification and Technical Requirements

The suite of 3-D Secure Specification and the Functional Requirements documents are designed to enable development by all Verified by Visa participants. Some 3-D Secure documents are available only to parties that have executed a license agreement, as noted below. To request a copy of the Visa Authenticated Payment Program License Agreement and licensed documents, send an email to <u>3DCompliance@visa.com</u>.

3-D Secure Publications:

- 3-D Secure Introduction (available on Visa.com)
- 3-D Secure System Overview (available on Visa.com)
- 3-D Secure Protocol Specification Core Functions (requires completed license agreement to access)
- 3-D Secure Functional Requirements Merchant Server Plug-in (requires completed license agreement to access)

3-D Secure Compliance and Testing Services

Acquirers or merchants that build or buy 3-D Secure Merchant Server Plug-in software will need to review the documents shown below. These documents require that the license agreement be completed:

- 3-D Secure Compliance Testing Facility Policies and Procedures
- 3-D Secure System and Compliance Testing Facility User Guide
- 3-D Secure System Test Facility Policies and Procedures

To obtain the license agreement and these documents, please send an email to Visa at: <u>3DCompliance@visa.com</u>.

For More Information

For more information about Verified by Visa or 3-D Secure, acquirers may visit Visa Online at <u>www.us.visaonline.com</u>. Click the *Products and Services* tab, then, click the "Verified by Visa" link.

1 Verified by Visa Overview

Verified by Visa is an online program designed to make Internet purchase transactions safer by authenticating a cardholder's identity at the time of purchase, before the merchant submits an authorization request. Verified by Visa software installed at the merchant's site activates the cardholder interface during the authentication process.

The goal of Verified by Visa is to create a level of consumer trust and confidence in online shopping similar to that in the physical shopping environment. It is designed to improve both cardholder and merchant confidence in Internet purchases and to reduce disputes and fraudulent activity related to the use of Visa payment cards. Merchants can benefit from reduced costs associated with the most common types of Internet disputes.

The Verified by Visa mark is displayed to the cardholder during activation and each time the cardholder enters a password for authentication at the time of purchase, and may also be displayed by participating merchants.

Verified by Visa is being implemented worldwide by Visa members and merchants.

1.1 Technology Platform

Verified by Visa is built upon the technology platform called Three-Domain (3-D) Secure, which is described beginning in Chapter 2, *3-D Secure Technology Platform* and Chapter 3, *Transaction Flows*.

1.2 Channels and Technologies Supported

Approved Channels for Verified by Visa Transactions

Verified by Visa is designed to support authentication for payment card transactions that originate electronically via the Internet. These transactions may be initiated by cardholders using a variety of Internet access devices.

Merchants **must not** use Verified by Visa for authentication for any orders that originate via mail, voice, or face-to-face interactions with the Visa cardholder. This includes a mail/telephone order or a customer making an online order that requires interaction with a merchant's customer service representative to complete the order. Cardholders **must not** be asked to verbally provide their Verified by Visa password. When the completion of a sale is facilitated by a merchant's customer service representative, the transaction **must** be processed as a telephone order transaction, not electronic commerce.

Technologies Supported

A wide variety of Internet access devices are supported by Verified by Visa, including personal computers and wireless devices, such as mobile phones when the phone is used as an Internet access device. Verified by Visa can operate with multiple authentication technologies including passwords, digital certificates, and chip cards. Merchant processing is independent of the authentication techniques adopted by the card issuer.

3-D Secure is designed to support both magnetic stripe and integrated circuit chip cards, for those countries where chip cards have been implemented. There are no additional requirements for Verified by Visa merchants when the card issuer authenticates a chip card or cardholder who is using a chip card.

1.3 Verified by Visa Overview

Verified by Visa enables real-time cardholder authentication by participating card issuers. With authentication, an issuer ensures that the presenter of the card is authorized and entitled to use the card. Online purchases are authenticated when the cardholder correctly enters the information requested by the issuer via the issuer's Access Control Server (ACS). Cardholders may activate their card a number of ways. If a U.S. issuer or cardholder has elected not to participate, Visa ensures that participating merchants receive "attempted authentication" responses.

Visa has modified the global operating regulations to shift chargeback liability for fraudulent consumer transactions from the acquirer and merchant to the issuer when a merchant submits proof that the transaction was authenticated – or the merchant *attempted to authenticate* – the cardholder in a Verified by Visa transaction.

Upon receiving an authentication response, merchants follow their standard electronic commerce procedures. After the status of order fulfillment is determined, the merchant formats a Visa authorization request which includes the required Verified by Visa authentication data and forwards the authorization request to its acquirer. The transaction is completed via traditional payment processing through VisaNet with authorization, clearing and settlement.

1.4 Authorization versus Authentication

While authorization and authentication are related, they are distinctly different processes with different business objectives:

• Authorization is the process used by a card issuer to approve or decline a Visa payment card transaction from a merchant or other card acceptor. Authorization request transactions most typically originate from a merchant's electronic point-of-sale terminal for card-present transactions. Card-not-present transactions, such as mail/telephone order or the Internet, are authorized electronically by the issuer based on payment card data that the merchant obtains from the cardholder. In both cases, the business objective of authorization is to provide a merchant with an approval or decline for a particular sale amount for a cardholder.

• Authentication is the process of the issuer validating the presenter's ownership of a Visa payment card. Authentication involves the issuer verifying a cardholder's pre-established Verified by Visa password or identity information provided by the cardholder.

Thus, authentication assures the card issuer that the presenter of the card is a valid card owner while authorization approves or declines the use of the card for a particular purchase transaction at a merchant.

1.5 Summary of Verified by Visa Benefits

Verified by Visa has been designed to benefit all participants in an online payment transaction. A summary of the benefits is shown below. Additional detail about merchant benefits is provided in Section 1.6, *Merchant Benefits*.

Benefits for Cardholders

- Increased consumer confidence for purchases via the Internet.
- No special application software is needed at the cardholder's access device.
- Ease of use.
- Control over card use for online purchases.

Benefits for Merchants

- Increased consumer confidence in online purchasing, potentially leading to increased sales volume.
- Reduced risk of fraudulent transactions.
- Reduced operational expense due to fewer transaction disputes.

Benefits for Issuers

- Reduces fraudulent transactions.
- Increased member online brand visibility because the issuer is involved in each transaction. This adds value and strengthens the issuer's relationship with the cardholder.
- Enables issuers to verify authentication data during Authorization Request processing.

Benefits for Acquirers

- Reduces fraudulent transactions.
- Reduces operational expense by decreasing the volume of chargebacks.
- Improved value to merchants through increased sales opportunities and decreased transaction disputes.

1.6 Merchant Benefits

Accepting payment cards for online payment can provide many opportunities for merchants, but may also present some challenges, including:

- Cardholder reluctance to purchase goods and services online because of the perception that purchasing is not secure.
- Costs associated with fraud by unauthenticated cardholders.
- Operational expenses associated with processing cardholder disputes.

Verified by Visa successfully addresses these issues and provides the benefits summarized in the following sections.

Increased Consumer Confidence

Consumer research indicates that payment card security concerns are a significant barrier to online purchasing, and that improved security would be a key motivator for increased online purchasing. Verified by Visa addresses security issues by enabling the issuer to authenticate cardholders during online purchases.

With improved security, cardholders who currently only browse the Internet will become more confident purchasers, thus, potentially increasing sales volume for participating merchants.

Fraud Reduction

When a Verified by Visa purchase transaction fails the authentication process, the merchant is alerted to the possibility of a potential fraud situation. The merchant **must not** submit the purchase for authorization if the authentication fails. Instead, the merchant may ask the cardholder for another form of payment. Verified by Visa helps reduce the fraudulent use of Visa cards at participating merchants.

Chargeback Protection

Participating in Verified by Visa provides protection for both authenticated and attempted authentication transactions, as described below:

- Authenticated Transactions. Since issuers authenticate cardholders' identities during Verified by Visa transactions, the following chargeback reason codes do not apply to successfully authenticated transactions*:
 - *Reason Code* 75 Cardholder Does Not Recognize Transaction
 - Reason Code 83 Fraud Transaction—Card Absent Environment
 - * Nоте:

Chargeback protection for authenticated transactions does not extend to merchants in four designated Merchant Category Codes; see Section 4.5, Merchant Type Exclusions. Additionally, merchants identified in monitoring programs for excessive chargebacks or fraud may not be eligible to submit authenticated transactions with ECI 5; see Section 11.2, Excessive Chargebacks and/or Fraud.

• Attempted Authentication Transactions. If a participating merchant attempts to authenticate a cardholder and either the issuer or cardholder is not participating in Verified by Visa, the merchant is provided with protection from chargebacks for the same reason codes as shown above for authenticated transactions. Merchants **must** properly process the 3-D Secure authentication messages and Visa authorization and settlement transactions to qualify for chargeback protection*.

* **N**оте:

Chargeback protection for attempted authentication transactions does not apply to the following: attempted authentications by Commercial or anonymous Prepaid cardholders and transactions conducted via New Channel devices. Merchants identified in monitoring programs for excessive chargebacks or fraud may not be eligible to submit attempted authentication transactions with ECI 6; see Section 11.2, Excessive Chargebacks and/or Fraud. Additionally, merchants in four designated Merchant Category Codes are not eligible for chargeback protection for attempted authentications; see Section 4.5, Merchant Type Exclusions.

Qualification for CPS/Electronic Commerce Preferred

Transactions may qualify for the Custom Payment Service (CPS)/Electronic Commerce Preferred fee programs that are shown below:

- CPS/Electronic Commerce Preferred Retail (Credit or Debit)
- CPS/Electronic Commerce Preferred Hotel and Car Rental (Credit or Debit)
- CPS/Electronic Commerce Preferred Passenger Transport (Credit or Debit)

CPS/Electronic Commerce Preferred includes authenticated and attempted authenticated transactions while CPS/e-Commerce Basic includes standard electronic commerce transactions. Only merchants that support Verified by Visa are eligible to qualify transactions for CPS/ Electronic Commerce Preferred.

Reduced Operational Expense

The customer service costs associated with dispute processing can be significant expenses to merchants. Even when disputed charges are successfully represented, exception item handling and dispute processing are costly. The reduction in fraud and operating expenses associated with the eliminated disputes gives merchants direct savings to their bottom line.

1.7 Merchant Marketing Opportunities

The Verified by Visa program sends a strong message to knowledgeable consumers that merchants that participate in the program are committed to conducting online sales in a secure manner. This creates the following marketing opportunities for participating merchants:

• Visa has developed a Verified by Visa mark for display on participating merchants' websites to promote consumer awareness and acceptance of the Verified by Visa program. The *Verified by Visa Merchant Toolkit* contains production-ready artwork and guides for usage of these program marks. See *About This Guide--Resources and Tools* for more information.



 Merchants may encourage buying instead of browsing by offering special promotions or exclusive offers to cardholders who purchase products and services using Verified by Visa. Enhanced security may have a positive influence on the consumer's initial purchasing experience and increase the likelihood of repeat business at the merchant's site.

2 **3-D Secure Technology Platform**

3-D Secure is a specification developed by Visa to improve transaction performance online and to accelerate the growth of electronic commerce. Verified by Visa is an authentication program based on the 3-D Secure Specification.

The 3-D Secure protocol is a technical platform that includes technical specifications and requirements for issuers, acquirers, and merchants. In addition to utilizing the widely supported Internet technology Secure Sockets Layer (SSL) encryption to protect payment card information during transmission over the Internet, 3-D Secure uses cardholder authentication to verify the parties involved in the transaction.

This section summarizes the roles of participants in the Verified by Visa program and provides a high level review of the 3-D Secure technology components.

For information about obtaining copies of the 3-D Secure Specification or Functional Requirements documents, see *About This Guide—Resources and Tools*.

2.1 3-D Secure Participants

Table 2-1 summarizes the roles of participants in the Verified by Visa program.

Participant Description	Role in Verified by Visa
Issuer: Financial institution that issues Visa cards to cardholders.	Manages cardholder participation and activation in Verified by Visa program; validates cardholder at the time of each online purchase; provides digitally signed response to merchant for each authenticated transaction. Issuers also have responsibility for the authentication experience of their cardholders.
Cardholder: Account holder of Visa payment card.	Uses card to pay for purchases over the Internet. Activates one time for Verified by Visa. Provides password at time of purchase.
Acquirer: Financial institution that contracts with merchants for acceptance of Visa payment cards.	Registers merchants for Verified by Visa; ensures that merchants originating Internet transactions are operating under a Merchant Agreement with the acquirer in accordance with the business rules and technical requirements for the Verified by Visa program.
Merchant: Offers merchandise or services at a website and accepts payment from a Visa cardholder who makes purchases over the Internet.	Operates software to support Verified by Visa program. This software is referred to as merchant server software or as a Merchant Server Plug-in (MPI). May develop and implement its own MPI or may obtain technology products and consulting services (including software integration into the merchant's commerce environment) from a technology provider. Participating merchants must display the Verified by Visa mark to communicate participation to their customers.
VisaNet: Systems and services, including the Verified by Visa Interoperability Domain, Visa Integrated Payments System and BASE II	Verifies issuer's authentication results. Routes authorization requests to issuers and sends responses to acquirers for return to merchants.

Table 2–1: Roles of Verified by Visa Program Participants

2.2 Software Components

The 3-D Secure Protocol divides the authentication process into three parts or "domains" according to the participants involved:

- Issuer Domain—Issuers, ACS processors and cardholders
- Acquirer Domain—Acquirers, gateway/merchant processors and merchants
- Interoperability Domain—Visa operated systems that connect the issuer and acquirer domains

Figure 2-1 illustrates the key participants and software components in each domain.

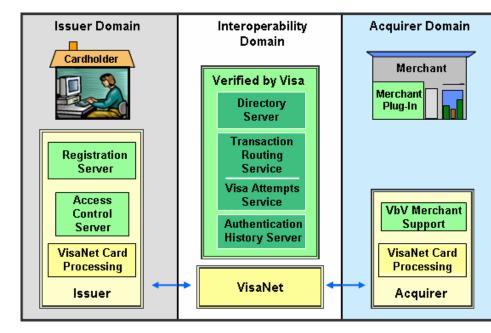


Figure 2-1: The Three Domains of 3-D Secure

Each domain is described further in the following sections.

The Issuer Domain

Issuer Registration Server (RS)

The Issuer Registration Server is the server that manages the cardholder registration/activation process. This server authenticates the cardholder for registration by presenting a series of questions to be answered by the cardholder and verified by the issuer, or by using a similar identity authentication process. The Registration Server is operated by the issuer or its ACS processor. The Registration Server is not necessarily a separate server. Registration functionality may be provided by the ACS processor.

Issuer Access Control Server (ACS)

The Access Control Server is a server with registered cardholder account and access information. The ACS is operated by the issuer or its processor. It validates cardholder participation in the program, performs cardholder verification at time of purchase, and provides digitally signed responses to merchants.

The Acquirer Domain

Merchant Server Plug-In (MPI, also referred to as Merchant Server Software)

A software module integrated into merchant websites, used to provide the interface between the Verified by Visa program and the merchant's payment processing software. The MPI may verify the issuer's digital signature used to sign authentication responses returned to the merchant, or this verification may be performed by a separate server, the acquirer, or a third party. The MPI also provides authentication data fields for inclusion in payment card authorization processing.

The Interoperability Domain

Visa Directory Server

A server operated by Visa to route authentication requests from merchants to issuers' Access Control Servers and to return the results of authentication.

Visa Transaction Routing Service (TRS)

All U.S. Verified by Visa authentication requests and responses are processed via the Visa Transaction Routing Service to ensure a timely response to merchants.

Visa Attempts Service

The Visa Attempts Service is an Attempts ACS (AACS) and provides attempted authentication responses to merchants when a cardholder or issuer is not enrolled in Verified by Visa or an issuer Access Control Server is not able to provide an authentication response. Additionally, the Visa Attempts Service provides stand-in processing when the issuer's ACS does not respond to an authentication request. The service is provided to U.S. participants in Verified by Visa. In case of a transaction dispute, the Visa Attempts Service provides proof that the merchant attempted to authenticate a transaction using Verified by Visa.

Authentication History Server (AHS)

A server operated by Visa to store data about authentication transactions. The Authentication History Server is used to verify authenticated transactions and to provide information during the dispute resolution process.

3 Transaction Flows

The Verified by Visa program includes two transaction flows for the cardholder:

- Cardholder enrollment or activation in the Verified by Visa program as described in Section 3.1, *Cardholder Enrollment/Activation*.
- Cardholder authentication during an online purchase at a participating merchant as described in Section 3.2, *Online Purchases*.

3.1 Cardholder Enrollment/Activation

Issuers may provide one or more of several enrollment options to their cardholders. Cardholders may enter a password that is used for authentication when shopping at the website of a merchant that participates in the Verified by Visa program or be authenticated by entering the requested information to verify their identity. Cardholders can also select a Personal Assurance Message that assures them that the password prompt window is actually from their card issuer.

This section provides a high-level look at common options for cardholder enrollment. Whatever form of enrollment is selected, the cardholder need only take a few minutes to complete the authentication steps.

Enrollment: Activation During Shopping

The most popular form of cardholder enrollment in Verified by Visa is known as "Activation During Shopping." This option facilitates a more targeted adoption rate and has helped enroll a critical mass of cardholders into Verified by Visa.

With Activation During Shopping, cardholders who have not set up their Verified by Visa password receive a request to do so when shopping at a participating merchant. The cardholder is presented with a series of security questions to be answered to verify the cardholder's identity. Once the identity is confirmed, the cardholder is asked to select a password.

Enrollment: Cardholder Registration

The second common form of enrollment is to give cardholders the option to visit a Verified by Visa website provided by the financial institution that issued their Visa card.

After cardholders enter their card number, they are presented with a series of security questions to be answered to verify the cardholder's identity. Once the identity is confirmed, the cardholder is asked to select a password and a Personal Assurance Message.

Enrollment: Registration Complete

After enrollment is complete, each time the cardholder makes an online purchase at a participating merchant's website, a Verified by Visa authentication page will appear to verify the identity of the cardholder, as described in Section 3.2, *Online Purchases*.

Alternative Cardholder Authentication Methods

Some issuers may use adaptive authentication in which the issuer dynamically determines the need for increased levels of authentication based on the cardholder's purchase patterns and characteristics of the particular transaction. For example, the issuer may elect to use an Activation During Shopping screen to require cardholder authentication, or to remove the Forgot Your Password option, when a purchase is determined to be higher risk, such as for a large amount or at a merchant where the cardholder has not previously shopped.

In most cases, Verified by Visa merchants will receive either an authenticated or an attempted authentication response along with the applicable chargeback protection.

3.2 Online Purchases

After enrolling as described in Section 3.1, the cardholder is ready to use Verified by Visa at any participating merchant.

Figure 3-1 illustrates the purchase transaction flow, which is described in the remainder of this section. Descriptions of each transaction step are in the sections that follow.

Step 1: Cardholder Finalizes Purchase

The cardholder browses at a participating merchant's website, adds items to the shopping cart, provides information required for checkout (by key entering data or by using an electronic wallet, a merchant one click service, or some other form-fill method), then clicks "Buy". The merchant now has all necessary data, including Primary Account Number (PAN) of the card presented for the purchase.

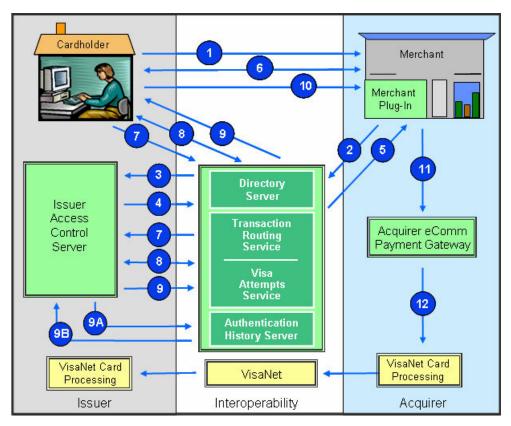
Note:

Steps 2-7 that follow are invisible to the cardholder.

Step 2: Merchant Server Plug-in Initiates 3-D Secure Processing

When the cardholder clicks Buy, the Merchant Server Plug-in (MPI) is activated. The MPI sends the PAN and other information to the Visa Directory Server to determine whether the card is in a participating range.

Figure 3–1: Purchase Transaction Flow



Step 3: Visa Directory Server Processes Request

The Visa Directory Server authenticates the merchant, as discussed in Chapter 8, *Digital Certificate Use*.

If merchant authentication is successful, the Visa Directory Server forwards the merchant query to the appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the card PAN.

If merchant authentication fails, the Directory Server returns an Error and the Verified by Visa transaction is terminated. If no appropriate ACS is available or the cardholder is not participating in Verified by Visa, the Visa Directory Server routes the request to the Visa Attempts Service which will process the authentication on behalf of the issuer.

Note:

In the case of where a Commercial card issuer is participating in Verified by Visa, the transaction will be routed to the issuer ACS. If the Commercial cardholder is enrolled in Verified by Visa, the cardholder will be authenticated and an ECI 5 transaction returned. If the Commercial cardholder is not enrolled, the ACS will return an attempted authentication response which the merchant will submit in the Authorization Request. In the Authorization Response, the CAVV Results Code value of **B** indicates that the transaction does not qualify for chargeback protection. If the Directory Server identifies a

Commercial card or anonymous Prepaid card with no assigned issued ACS, a Verify Enrollment Response of U will be returned to indicate that these cards are not subject to Verified by Visa business rules related to attempted authentications.

Step 4. ACS Responds to Visa Directory Server

The issuer ACS, or Visa Attempts Service if an issuer ACS is not available, determines whether authentication is available for the card's PAN, prepares a response, and sends it to the Visa Directory Server.

Step 5: Visa Directory Server Returns Response

The Visa Directory Server returns the ACS response (or its own) to the MPI.

If authentication is available, the response includes the URL of the Visa Transaction Routing Service and the issuer ACS to which the merchant will send the Payer Authentication Request.

Step 6: MPI Sends Payer Authentication Request

If authentication (or proof of an attempted authentication) is not available, then the MPI advises the merchant commerce server that authentication is not available, and processing continues with Step 12.

The MPI sends the Payer Authentication Request to the ACS via the Visa Transaction Routing Service via the cardholder's device (PC browser or other device), using the URL received in Step 5. The Payer Authentication Request contains information about the purchase transaction.

Step 7: ACS Receives Payer Authentication Request

The Visa Transaction Routing Service receives the Payer Authentication Request and forwards it to the appropriate issuer ACS.

Step 8: ACS Authenticates Cardholder

The ACS formats an authentication request for the cardholder. The authentication request is returned via the Visa Transaction Routing Service to the cardholder's browser. The cardholder may be authenticated using processes applicable to the PAN (password, Activation During Shopping, etc.). For authentication by password, an example Verified by Visa password screen is shown in Figure 3-2:

- After clicking Buy in Step 1, the cardholder sees a window that contains purchase details and that prompts the cardholder to provide his or her Verified by Visa password.
- The cardholder enters their password and clicks Submit.
- The ACS determines whether the provided password is correct.

The ACS formats a Payer Authentication Response with appropriate values, including authentication status and, if applicable, Electronic Commerce Indicator (ECI) and Cardholder

Authentication Verification Value (CAVV). The CAVV is used to confirm that an authentication, or proof of an attempted authentication, was conducted.

The ACS signs the Payer Authentication Response with the issuer's Verified by Visa Signature Key. This key allows the merchant to verify that the response originated from a valid participating issuer and that the message was not tampered with on route.

Figure 3–2: Verified by Visa Password Entry Screen

Verified by Visa	- 🗆 ×
Verified by VISA My Issuing Bank Lo	go
Added Protection Please submit your Verified by Visa password.	
Merchant: merchant.com	
Amount: \$49.16	
Date: 09/01/2010	
Card Number: **** **** 9010	
Personal Message: Cardholder since 05/2000	
Password: Forgot your password? Submit ? Help	E <u>xit</u>
Inter	rnet //

Step 9: ACS Returns Authentication Results

The ACS returns the signed Payer Authentication Response to the Visa Transaction Routing Service which forwards the response to the MPI via the cardholder's device.

- **Step 9A**: Whether or not authentication was successful, the ACS sends a copy of the Payer Authentication Response, including related data, to the Authentication History Server.
- **Step 9B**: The Authentication History Server provides an acknowledgment response that the Payer Authentication Response transaction data was received.

The Authentication History Server serves as the database of record for dispute resolution.

Step 10: MPI Receives Payer Authentication Response

The cardholder's device forwards the signed Payer Authentication Response to the MPI.

Step 11: MPI Processes Response

The MPI validates the signature on the Payer Authentication Response along with other data in the response.

The MPI, then, passes the results of the authentication attempt to the merchant commerce server.

Step 12: Authorization Processing

Based on the data received from the MPI, the merchant commerce server determines whether to proceed with authorization, as described in Chapter 5, *Authorization Processing*.

If the merchant commerce server advises the MPI that authentication failed, the merchant should request another form of payment from the shopper.

If authorization is appropriate:

- The merchant commerce server sends an authorization request to the merchant's acquirer or merchant payment processor. The authorization request includes the Electronic Commerce Indicator (ECI) appropriate to the authentication status and the CAVV, when required.
- The acquirer sends the authorization request, including Verified by Visa authentication information, to the issuer via VisaNet.
- The issuer receives and processes the authorization request. When the CAVV is passed in BASE I, either the issuer or Visa on the issuer's behalf, will perform CAVV verification. The issuer returns an authorization response. The issuer may choose to approve or to decline the authorization request for reasons unrelated to the Verified by Visa authentication (e.g., insufficient funds, closed account, etc.).
- If the issuer authorizes the transaction, the merchant displays an order confirmation as usual, providing the cardholder with details about the order, delivery, and the merchant's customer service.

4 **3-D Secure Messages**

This chapter briefly describes each 3-D Secure message involving the Merchant Server Plug-in (MPI). Please refer to 3-D Secure: Protocol Specification – Core Functions for additional detail about these messages (see About This Guide—Resources and Tools).

4.1 Verify Enrollment Messages

Upon the completion of checkout, the merchant server software formats a message to the Visa Directory Server to determine whether the shopper's card is activated in Verified by Visa.

Table 4-1 describes the types of Verify Enrollment messages.

Message Type	Description
Verify Enrollment Request (VEReq)	The merchant server software sends the VEReq message to the Visa Directory Server which forwards the request to the appropriate issuer ACS to determine whether a particular card number is enrolled and can be authenticated.
Verify Enrollment Response (VERes)	The Visa Directory Server returns the VERes message to the MPI, indicting whether the cardholder participates in Verified by Visa (as described in Table 4-4).
Error message	The merchant was unable to provide the appropriate credentials to the Directory Server (see Table 4-2 for the applicable error codes).

Table 4–1:Verify Enrollment Messages

The possible Verify Enrollment Response values are shown in Table 4-2.

 Table 4–2:
 Verify Enrollment Response Values

Message Type	Response Value
Verify Enrollment Response (VERes)	The Visa Directory Server returns the VERes message, indicating one of the following: \mathbf{Y} = Authentication Available – Cardholder is enrolled, Activation During Shopping is supported, or proof of attempted authentication available. The merchant uses the URL of issuer ACS included in VERes to create the Payer Authentication Request. \mathbf{N} = Cardholder Not Participating – Cardholder is not enrolled. \mathbf{U} = Unable to Authenticate or Card Not Eligible for Attempts (such as a Commercial or anonymous Prepaid card).

Table is continued on the next page.

Table 4–2:	Verify Enrollment Response Values (Continued)
------------	-----------------------------------------------

Message Type	Response Value
Error message	The merchant was unable to provide the appropriate credentials to the Directory Server. The related error codes are: 50 – Acquirer not participating 51 – Merchant not participating 52 – Password Missing 53 – Incorrect password 54 – Incorrect Common Name value in Client Certificate Note: An error message may also be returned for other reasons, such as a field that is formatted incorrectly.

U.S. versus International Verify Enrollment Responses

The differences in Verified by Visa processing as described below:

- For **U.S. Consumer Transactions**, Visa provides authentication responses when a participating Verified by Visa merchant attempts to authenticate a cardholder, when either the cardholder or the issuer does not yet participate in Verified by Visa.
 - The Directory Server forwards the transaction to the Visa Attempts Service, which will return a Y in the VERes message.
 - If the card is not eligible for Verified by Visa (e.g., most Commercial cards), the VERes message will contain a value of U for unable to authenticate. If a VERes U response is received, the merchant proceeds with the transaction as an ECI 7.
 - While merchants will receive a VERes of Y or U for most U.S. transactions, it is possible that a merchant will receive a VERes of N for a non-enrolled U.S. cardholder or a nonparticipating U.S. issuer BIN. In these cases, merchants should submit the Visa Authorization Request with an ECI 6 even though no CAVV is available. If the cardholder later disputes the transaction, the merchant will be able to use their Verified by Visa logs to demonstrate that authentication was attempted.
- For **International Consumer Transactions**, non-U.S. issuers may optionally support responses to attempted authentications, returning a **Y** in the VERes message.
 - Other non-U.S. issuers, especially those not yet participating in Verified by Visa, will not have the capability to support attempts responses. In these transactions, participating merchants will receive a VERes response of **N** for non-enrolled cardholder or non-participating issuer. For these transactions, the merchant submits the Visa Authorization Request with an ECI of **6**, leaving CAVV blank. VisaNet recognizes the issuer as non-U.S. and permits these transactions to qualify for chargeback protection even though there is no CAVV included in the authorization.
 - Merchants will also receive a VERes of U for non-U.S. accounts that are not eligible for chargeback protection of attempted authentications. Again, if a VERes U response is received, the merchant proceeds with the transaction as an ECI 7.

4.2 Payer Authentication Messages

Upon receiving a Verify Enrollment Response (VERes) indicating that authentication is available, the merchant server software formats a Payer Authentication Request (PAReq) and forwards it to the Visa Transaction Routing Service and issuer ACS whose URL was included in the VERes, via the cardholder's browser or device. Table 4-3 describes these messages.

Note:

In the VERes message returned by the issuer, the PAN Authentication Available field had the value "Y" (indicating "Authentication Available") and all other fields passed all required edits.

Message Type	Description
Payer Authentication Request (PAReq)	The merchant server software sends the PAReq message to the issuer ACS to request cardholder authentication. The PAReq contains cardholder, merchant, and transaction-specific information.
	Note : The Merchant Name used in the PAReq message must exactly match the Card Acceptor Name (field 43) in authorization requests and the Merchant Name field in BASE II (TC05, TCR0, positions 92 116).
Payer Authentication Response (PARes)	The issuer ACS returns the PARes message, including the issuer's authentication decision (as described in Table 4-4).
Error message	The PAReq could not be processed because, for example, a field was formatted incorrectly.

Table 4–3: Payer Authentication Messages

Table 4-4 lists the possible outcomes when the issuer ACS authenticates the cardholder, and the codes used to communicate the issuer's authentication decision. The values displayed are those inserted in the "Transaction Status" field of the Payer Authentication Response message that is returned to the merchant.

Table 4–4: Issuer Authentication Results Values

Authentication Result Determined by Issuer ACS	Transaction Status Values
Authentication Successful The issuer has authenticated the cardholder by verifying the password or other identity information.	Y
Attempts Processing Performed Authentication was not available, but functionality was available (through the issuer, the Visa Attempts Service, or a third party) to generate a proof the merchant attempted VbV authentication.	Α
Authentication Failed The cardholder's password (or other authentication information) failed validation, thus, the issuer is not able to authenticate the cardholder. The following are reasons to fail an authentication: Cardholder fails to correctly enter the authentication information within the issuer-defined number of entries (possible indication of fraudulent user). Cardholder "cancels" authentication page (possible indication of a fraudulent user). Merchants are not permitted to submit these transactions for authorization processing.	N
Authentication Could Not Be Performed The issuer ACS is not able to complete the authentication request – possible reasons include: Card type is excluded from attempts (such as a Commercial Card or an anonymous Prepaid Card) ACS not able to handle authentication request message ACS is not able to establish an SSL session with cardholder browser System failure that prevents proper processing of the authentication request Merchants may proceed with the above purchases as non-authenticated and retain liability if the cardholder later disputes making the purchase. These are non-Verified by Visa electronic commerce transactions. When the PARes has a U and an Invalid Request Code of 55, this indicates that the Account Identifier in the PAReq did not match the value returned by the ACS in the VERes. Merchants must view this as an invalid transaction.	U

Upon receiving the Payer Authentication Response, the merchant server software uses the Transaction Status field (and other data) to determine whether it is appropriate for the merchant commerce server to submit an authorization request, as described in Chapter 5, *Authorization Processing*.

4.3 Handling of the Merchant Password Field in 3-D Secure Messages

Since U.S. merchants are authenticated to the Visa Directory Server via merchant certificates, there is no need for U.S. merchants or merchant processors to include the password tag or password value in the XML format of 3-D Secure messages for a Verify Enrollment Request. This means that both the password tag and password value may be omitted from U.S. 3-D Secure messages.

Note:

Acquirers or merchant processors that also support merchants outside of the U.S. where passwords may be used for merchant authentication should check the Verified by Visa Acquirer Guide for the Region in which the merchants are located.

4.4 Attempted Authentication Exclusions

The Visa Operating Regulations specify that several types of transactions that are excluded from requirements for attempted authentications:

- Excluded Card Types Two card types, Commercial cards and anonymous Prepaid cards, are excluded from requirements for attempted authentications on non-enrolled cardholders. The Visa Directory Server will verify that the BIN is an excluded card type and return U in the Verify Enrollment Response to the merchant to communicate that attempted authentications do not apply.
- New Channel Devices Transactions originated with Visa-designated new channel device types.
- Merchants identified in monitoring programs for excessive chargebacks or fraud are not eligible to submit authenticated and/or attempted authentication transactions. See Section 11.2, *Excessive Chargebacks and/or Fraud*, for more information.

The Verify Enrollment response for these transactions will be a **U** to indicate that the transaction is not eligible for attempts processing. These transactions are standard electronic commerce and are submitted in the Visa Authorization Request with an ECI of **7** as CPS/e-Commerce Basic, as outlined in Chapter 5, *Authorization Processing*.

4.5 Merchant Type Exclusions

There are four Merchant Category Codes (MCCs) for which U.S. merchants retain chargeback liability when U.S. cardholders are either authenticated with Verified by Visa or there is an attempted Verified by Visa authentication. These four Merchant Category Codes are:

- Wire Transfer/Money Order (MCC 4829)
- Direct Marketing-Inbound Teleservices (MCC 5967)
- Non-Financial Institution-Foreign Currency, Money Order (not Wire Transfer), Travelers' Cheques (MCC 6051)
- Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting and Wagers at Race Tracks (MCC 7995)

If a cardholder disputes a transaction as not conducted by him/her, the issuer may submit a chargeback for Reason Code 75 (Cardholder Does Not recognized Transaction) or Reason Code 83 (Fraud Transaction – Card Absent Environment). The acquirer may not represent these chargebacks even if the transaction was authenticated or an attempted authentication.

The chargeback liability for the above four MCCs **does not** apply to international transactions where either the cardholder or merchant is non-U.S.

See Chapter 12, *Dispute Resolution*, for more information.

4.6 Cache Messages

Important Notice for Acquirers and Merchants:

Use of a cache to maintain lists of card ranges is **not permitted for U.S. merchants** as the Visa Directory Server contains the most current, full listing of all Visa card ranges. As a result, U.S. merchants **must not** implement support for Cache Update Request or Cache Update Response messages.

5 Authorization Processing

Upon receiving the Payer Authentication Response, the merchant's MPI:

- Validates the issuer's digital signature using the Visa 3-D Secure Root Certificate, and
- Validates other fields in the Payer Authentication Response as described in the document 3-D Secure: Protocol Specification – Core Functions.

The MPI notifies the merchant commerce server if either validation fails. These transactions are treated as though authentication had failed. The merchant should then request another form of payment from the shopper. A merchant **must not** submit a failed authentication transaction for authorization.

If both validations are successful, then the MPI reviews the value in the Transaction Status field of the Payer Authentication Response (PARes) message to determine the payment authentication results, and passes the results to the merchant commerce server, along with the Electronic Commerce Indicator (ECI) and Cardholder Authentication Verification Value (CAVV), if received. More information on both ECI values and CAVV is provided in sections that follow.

Table 5-1 lists the Transaction Status field values and appropriate merchant authorization processing for each.

Results of Authentication Attempt	Transaction Status	Merchant Response
Authentication Successful	Y	The merchant submits an authorization request including the ECI and CAVV supplied in the PARes.
Attempts Processing Performed	Α	The merchant submits an authorization request including the ECI and CAVV supplied in the PARes.
Authentication Failed	N	The merchant must not submit a failed authentication for authorization.
Authentication Could Not Be Performed	U	The merchant may process an authorization request using the appropriate ECI. See "3-D Secure Response Mapping Exhibit" in Table 5-2 for additional information.

Table 5–1: Transaction Status Values

5.1 Electronic Commerce Indicator (ECI)

The Electronic Commerce Indicator (ECI) indicates the level of security used when the cardholder provided payment information to the merchant. It **must** be set to a value corresponding to the authentication results and the characteristics of the merchant checkout process. The merchant commerce server transmits the authorization request message, including the ECI, to the acquirer or its processor.

Possible ECI data values are:

- ECI = 5: This value means that the cardholder was authenticated by the issuer by verifying the cardholder's password or identity information. The value is returned by the ACS in the Payer Authentication Response message when the cardholder successfully passed 3-D Secure payment authentication.
- **ECI = 6:** This value means that the merchant attempted to authenticate the cardholder, but either the cardholder or issuer was not participating. The value should be returned by the ACS in the Authentication Response message for an Attempt Response. Additionally, merchants may use an ECI **6** in the authorization request when a Verify Enrollment of **N** is received from the Visa Directory Server.
- ECI = 7: This value is set by the merchant when the payment transaction was conducted over a secure channel (for example, SSL/TLS), but payment authentication was not performed, or when the issuer responded that authentication could not be performed. An ECI 7 applies when either the Verify Enrollment or the Payer Authentication Response contains a **U** for Unable to Authenticate.

These values and related information are summarized in Section 5.3, *Authentication and Authorization*.

Electronic Commerce Indicator Restrictions

U.S. merchants that have been identified in monitoring programs for excessive chargebacks or fraud may not be eligible to submit authenticated (ECI **5**) and/or attempted authentication (ECI **6**) transactions; see Section 11.2, *Excessive Chargebacks and/or Fraud* for more information.

Note:

ECI values in BASE I are two digits, the number shown above with a leading zero. ECI values in the Single Message System and in BASE II are single digits as shown above.

Important Notice:

Merchants **must** submit the correct ECI value, as defined in Table 5-2 in both the authorization request and the clearing/settlement record, to ensure liability protection.

The Visa Operating Regulations specify penalties for acquirers whose merchants fail to provide the correct Electronic Commerce Transaction indicator values.

5.2 Cardholder Authentication Verification Value and Authentication Identifier

Cardholder Authentication Verification Value (CAVV)

The CAVV is a cryptographic value derived by the issuer during authentication that can provide evidence of the results of payment authentication during an online purchase. If a merchant receives a CAVV value in a Payer Authentication Response message from the issuer, the CAVV **must** be included in the VisaNet authorization message in order for the merchant to receive chargeback protection for U.S. and international transactions:

- The merchant **must** be able to send the CAVV to its acquirer.
- The acquirer **must** be able to receive the CAVV from the merchant and correctly transmit the data in the authorization request.

Authentication Identifier

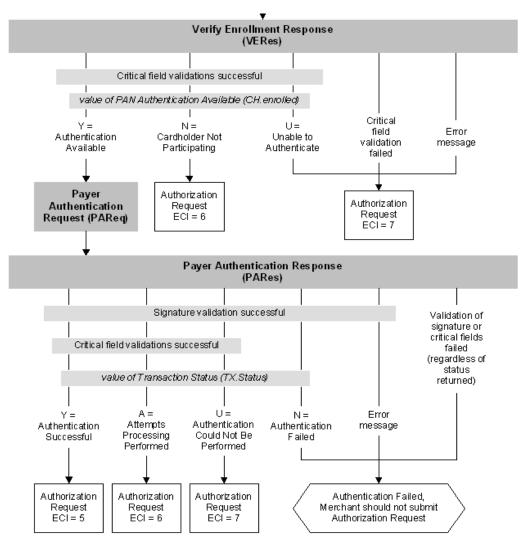
.

The Authentication Identifier is the Authentication Tracking Number (ATN) subfield of the CAVV value transmitted by the issuer ACS. Acquirers and merchants are not required to transmit a separate Authentication Identifier

5.3 Authentication and Authorization

Figure 5-1 summarizes the possible outcomes of a Verified by Visa transaction, illustrating when a merchant's submission of an authorization request is permitted.

Figure 5–1: Determining Whether to Submit Authorization



3-D Secure Response Mapping to Authorization

Table 5-2 specifies the relationships between Verified by Visa processing scenarios, the presence/absence of CAVV and ECI values.

Field Explanations for Table 5-2:

- **VE Response**: The value of the PAN Authentication Available field in the Verify Enrollment Response (VERes) message.
- **PA Response**: The value of the Transaction Status field in the Payer Authentication Response (PARes) message.
- **PA ECI**: An ECI value assigned by the issuer (based on the outcome of the interaction between cardholder and issuer) and passed to the merchant in the PARes message. An ECI is not included in this message when the Transaction Status equals 'U'.
- VisaNet ECI: The ECI value that should be submitted by the merchant/acquirer in VisaNet. To ensure chargeback protection for the merchant the correct ECI for the transaction **must** also be submitted in the clearing and settlement record.

Response to Authentication Request	VE Resp	PA Resp	PA ECI	CAVV in PARes	CAVV in BASE I	ECI in BASE II / Settlement
Authentication Confirmation Scenario: Participating issuer, participating cardholder Enrollment verified; authentication successful	Y	Y	5	Yes Yes No	Yes No N/A	5 7 7
Attempted Authentication Scenario: Cardholder shopping at a merchant. An attempts ACS acts on behalf of non-participating issuers and non enrolled cardholders	Y	A	6	Yes	Yes No	6 7
Denial Scenario: Participating issuer, participating cardholder Enrollment verified; but issuer not able to authenticate cardholder	Y	N	N/A	No	N/A	N/A (Authorization request must not be submitted)

Table 5–2: 3-D Secure Response Mapping Exhibit

Table is continued on the next page.

Response to Authentication Request	VE Resp	PA Resp	PA ECI	CAVV in PARes	CAVV in BASE I	ECI in BASE II / Settlement
Non-Participation Scenario 1: Non-participating issuer Scenario 2: Participating issuer, card range associated with cardholder not registered at Visa Directory Server Scenario 3: Participating issuer, cardholder not enrolled at ACS	N	None	N/A	N/A	N/A	6
Unable to Authenticate (a) Scenario: Participating issuer, participating cardholder Enrollment verified successfully. ACS, however, does not respond to the PAReq with the necessary PARes. Incomplete transaction	Y	None	N/A	N/A	N/A	7
Unable to Authenticate (b) Scenario: Participating issuer, participating cardholder Enrollment verified successfully. ACS, however, cannot match account ID in PAReq with the value assigned in corresponding VERes. Questionable transaction NOTE: If ACS processing uses single-use account IDs, condition may indicate replay condition	Y	U	N/A	No	N/A	7
Unable to Authenticate (c) Scenario 1: Participating issuer. ACS is not able to verify enrollment status of cardholder because the card type (e.g., commercial card or anonymous prepaid card) or new channel is not supported Scenario 2: Non-participating issuer, ineligible product	U	None	N/A	N/A	N/A	7

Table 5–2: 3-D Secure Response Mapping Exhibit (Continued)

5.4 PARes Fields for Authorization Requests

For each transaction for which an authorization request may be submitted (as discussed in Section 5.3, *Authentication and Authorization*), the MPI is required to pass the PARes fields listed in Table 5-3 to the merchant commerce server in order to correctly identify the transaction in the authorization process.

Table 5–3: PARes Fields Required for Authorization Messages

PARes Field Name	PARes DTD Element	See Sections	
Electronic Commerce Indicator	TX.eci	5.1	
Cardholder Authentication Verification Value	TX.cavv	5.2, 5.3, and 5.4	

Transmit CAVV Without Modification

The MPI receives the PARes as a Base64-encoded message. The CAVV field within the PARes message, if present, has been separately Base64 encoded, resulting in a 28-byte value. To adhere to the VisaNet requirements for Field 126.9, which is 20 bytes long, the CAVV **must** be decoded into a 20 byte binary value prior to submitting it to VisaNet.

The following sequence is therefore necessary:

- The MPI Base64 decodes the PARes message and performs signature validation and field validation as required.
- If the CAVV is present, the MPI passes it, as received, to the merchant commerce server.
- The merchant commerce server or the merchant processor:
 - Base64 decodes the CAVV field to get it back to a 20 byte binary value
 - If necessary, converts the data field to the gateway processor's traditionally required data format (EBCDIC, etc.)
 - Submits the data field to the gateway processor or the acquirer
- The gateway processor or the acquirer constructs the BASE I authorization message to ensure that the CAVV is entered in BASE I as a binary value in Field 126.9.

Important Notice:

Merchants should contact their Visa acquirer with any questions about CAVV processing.

5.5 Electronic Commerce Custom Payment Service Qualification

Custom Payment Service (CPS) Programs establish a framework for processing transactions across different acceptance environments. There are requirements for defined data fields, processing rules, interchange rates and chargeback provisions. The CPS/Electronic Commerce categories are highlighted below.

Note:

For information regarding CPS programs, merchants should contact their Visa acquirer to ensure that processing requirements are met.

CPS/Electronic Commerce – Basic (Credit or Debit)

The CPS/Electronic Commerce – Basic program applies to retail merchants that process ecommerce transactions and Select Developing Market transactions. The transaction is a nonauthenticated, secure electronic commerce transaction that requires the appropriate ECI and may require an AVS. Note: There are other requirements for this CPS program.

CPS/Electronic Commerce Preferred – Retail (Credit or Debit)

In a CPS/Electronic Commerce Preferred – Retail transaction, the transaction takes place in a secure Internet environment utilizing Verified by Visa. The cardholder transaction may be authenticated or an attempted authentication. The appropriate ECI and CAVV are required and AVS may be required. Note: There are other requirements for this CPS program.

CPS/Electronic Commerce Preferred – Hotel and Car Rental (Credit or Debit)

For CPS/Electronic Commerce Preferred – Hotel and Car Rental, the transaction takes place in a secure Internet environment utilizing Verified by Visa. The cardholder transaction may be authenticated or an attempted authentication. The appropriate ECI and CAVV are required. Note: There are other requirements for this CPS program.

CPS/Electronic Commerce Preferred – Passenger Transport (Credit or Debit)

In a CPS/Electronic Commerce Preferred – Passenger Transport transaction, the transaction takes place in a secure Internet environment utilizing Verified by Visa. The cardholder transaction may be authenticated or an attempted authentication. The appropriate ECI and CAVV are required. Note: There are other requirements for this CPS program.

Acquirers may obtain information about Customer Payment Service program qualification in the U.S. Interchange Reimbursement Fee Rate Qualification Guide that is available via Visa Online.

5.6 ACI and ECI Values Must Be Consistent

For U.S. transactions, an Authorization Characteristic Indicator (ACI) will be returned by VisaNet in the Authorization Response. The ACI is required to be submitted in the clearing and settlement message. And, the ACI submitted by the acquirer for settlement **must** be consistent with the ECI that is also submitted in the clearing and settlement messages. The ACI indicates the CPS category for which the transaction qualifies, as shown in Table 5-4.

ACI Value in Authorization Response	What the Value Means	ECI Value for Settlement
U	Transaction qualified as CPS/Electronic Commerce Preferred as an authenticated purchase.	5
S	Transaction qualified as CPS/Electronic Commerce Preferred as an attempted authentication.	6
W or P	Transaction qualified as CPS/Electronic Commerce Basic as a standard electronic commerce transaction.	7

 Table 5–4:
 ACI and ECI Values for Authorization Messages

5.7 No Re-Use of Authentication Data

Authentication data for a transaction **must not** be submitted in the Authorization Request for another transaction. There are two exceptions to this general requirement. One is for split shipments and the other is for delayed delivery, as explained below:

- **Split Shipment**: A split shipment occurs when a single purchase order results in more than one shipment of merchandise. In the event a merchant splits the shipment of an order, the second Authorization Request may be submitted with the original authentication data for the purchase.
- **Delayed Delivery**: When a second Authorization Request is submitted for the same original purchase due to delayed delivery, the authentication data may be included in the second Authorization Request message.

In the event of a cardholder dispute, the acquirer and merchant **must** be able to demonstrate that all Authorization Requests are related to the single, original, authenticated purchase transaction. The total amount of the split transaction **must not** exceed 15% over the original authentication amount. The 15% variation allows for shipping costs associated with the items. Any authorization amount that exceeds 15% of the authenticated amount is not subject to Verified by Visa chargeback protection and may be charged back by the issuer.

5.8 Recurring Transactions

Recurring transactions occur when the cardholder and merchant agree to purchase goods or services on an ongoing basis over a period of time. Recurring transactions are multiple transactions processed at predetermined intervals, not to exceed one year between transactions. Examples of recurring transactions include insurance premiums, subscriptions, Internet service provider fees, membership fees, tuition, or utility charges.

To qualify for Verified by Visa chargeback protection, the first transaction in the series **must** be authenticated and **must** follow authorization rules associated with an authenticated transaction, which means the authorization is submitted with the appropriate ECI and CAVV for the Verified by Visa transaction.

All subsequent authorization requests in the recurring series **must** be processed as Recurring Transactions, using the Recurring Indicator (MOTO/ECI value of **2**). The merchant **must not** store and submit the CAVV with any subsequent authorization transaction.

Because the first transaction was conducted via the Internet as a Verified by Visa authenticated or attempted authentication, chargeback protection applies to the original electronic commerce transaction. For the subsequent Recurring Transactions, chargeback provisions applicable to Recurring Transactions apply; Verified by Visa chargeback protection does not apply.

Note:

The 'Recurring Payment Data' field, 'Recurring Frequency' field, and 'Recurring Expiry' field in the Payer Authentication Request message are required when the merchant and cardholder have agreed to recurring payments. The 'Recurring Expiry' field must contain a date that is later than the original authentication date.

5.9 Installment Transactions

Like recurring transactions, installment transactions are divided into two or more transactions and are billed to an account in multiple segments over a period of time that is agreed to by the cardholder and merchant. However, the transaction is for a single good or service rather than an ongoing (or recurring) purchase. The transactions **must** have a specified end date. Similar to the processing of recurring payments, the initial installment transaction **must** be authenticated and **must** follow authorization rules associated with an authenticated transaction. The remaining transactions are processed as installment transactions, so **must not** contain authentication data, specifically the ECI and the CAVV. Chargeback liability protection for the acquirer/merchant does not apply to the subsequent installment transactions.

Note:

The 'Installment Payment Data' field in the Payer Authentication Request message is required when the merchant and cardholder have agreed to an installment payment option.

5.10 Online Auctions

Participating merchants that offer online auctions may submit a valid CAVV and appropriate ECI for an authentication or attempted authentication transaction in the Authorization Request message, even though the purchase amount may have changed from the Payer Authentication Request (PAReq) to the Authorization Request. Merchants **must not** re-use the CAVV for another transaction with the same cardholder (for example, on another auction).

5.11 Authentication Data Limits

Time Limit

Data received in an original authentication may be obtained up to **90 days prior to** an authorization date. This time allows for instances such as pre-purchase transactions where the cardholder may pre-order and purchase a good or service prior to the item's availability in the market.

Amount Variation

The original authentication data will be valid in authorization for amounts that do **not exceed 15%** over the authenticated amount. This variation allows for additional shipping costs associated with the transaction.

6 Merchant Server Plug-In Functions

This section describes the functions of the Merchant Server Plug-in (MPI) in Verified by Visa. The MPI may be software that can be integrated with a merchant's Internet storefront software or may be supplied as a service by an acquirer, payment service provider, payment gateway provider, or Internet Service Provider (ISP). For more information, see Chapter 9, *MPI Implementation Options*.

The primary functions of the MPI are:

- To ascertain whether 3-D Secure authentication is available for a particular cardholder
- To submit requests for payment authentication
- To validate the digital signature in the ACS Payer Authentication Response message
- To provide authentication information to the merchant commerce server
- To store Payer Authentication Response data

6.1 Message Processing Functions

The MPI **must** perform the following message processing functions.

Verify Enrollment Requests/Responses

- Format Verify Enrollment Request (VEReq) messages and send them to the Visa Directory Server.
- Receive and process Verify Enrollment Response (VERes) messages from the Visa Directory Server.

Payer Authentication Requests/Responses

• Format Payer Authentication Request (PAReq) messages and send them to the ACS via the cardholder's device and the Visa Transaction Routing Service.

Important Notice for Acquirers and Merchants:

The Merchant Name used in the PAReq message **must** exactly match the Card Acceptor Name (field 43) in authorization requests and the Merchant Name field in BASE II (TC05, TCR0, positions 92 116).

- Receive Payer Authentication Response (PARes) messages from the ACS via the cardholder's device.
- Use the Visa 3-D Secure Root Certificate to validate the cryptographic signature in the PARes message to ensure its authenticity and integrity.
- Otherwise process PARes messages.

• Provide authentication results data to the merchant's authorization processing function.

Error Messages

• Format, send, receive, and process error messages as required.

Card Range Request/Responses and Caching

Important Notice for Acquirers and Merchants:

All Visa card ranges are supported in the Visa Directory Server. U.S. merchants and merchant processors **are not** permitted to support a Card Range Cache and use CRReq/CRRes messages. Instead, all U.S. merchant MPIs **must** forward Verify Enrollment Request messages to the Directory Serve. This will ensure the highest accuracy for Verified by Visa processing.

6.2 Additional MPI Functional Requirements

Client Digital Certificates and Visa 3-D Secure Root Certificate

Merchant certificates **must** be encrypted and securely stored in the merchant's systems for access by the MPI. The MPI **must** also be able to import and securely store the Visa 3-D Secure Root certificate. See Chapter 8, *Digital Certificate Use*, for additional information on merchant certificates.

Record Keeping

The MPI must log all Verified by Visa related functions as part of normal processes.

The MPI **must** be able to store and retrieve PARes records and associated PANs for dispute resolution purposes. (See Chapter 12, *Dispute Resolution*, for more information.)

Note:

These functions may instead be performed by the merchant commerce server, if it receives the data from the MPI.

Reporting

It is highly desirable that the MPI (or the merchant commerce server) enable merchants to create reports on individual Verified by Visa transactions. Reports on this data can be important for operational monitoring and dispute resolution staff.

Recommended reports include:

- Successfully authenticated transactions by Transaction ID, PAN, Invoice Number, Month, Date, or Date Range
- Transactions with point of failure information by Transaction ID, PAN, Invoice Number, Month, Date, or Date Range

Data elements for reports: It is highly desirable that merchants modify current transaction reporting to include Verified by Visa specific fields. This following data will be beneficial in disputes resolution:

- Transaction Status (results of authentication Y, A, U, or N)
- Electronic Commerce Indicator (ECI 5, 6, or 7)
- CAVV Field (includes the Authentication Tracking Number or ATN to assist research with CAVV Field in Visa Authorization Request message

Monitoring

The merchant (or its hosting entity) **must** integrate monitoring of the MPI server and application into its systems monitoring processes so that the merchant can quickly identify and correct problems with its implementation of 3-D Secure. Quick identification and repair will enable the merchant to minimize any potential loss of the program benefits on its Visa transactions, and participating cardholders will be more likely to have the Verified by Visa experience they have grown to expect at a Verified by Visa merchant.

Note:

The merchant (or its hosting entity) **must not** send test transactions to the Visa Directory Server as part of its monitoring.

Directory Server Fallback

Merchants **must** implement fallback to a secondary Visa Directory Server. Merchants should consult with their MPI software vendor to identity the correct primary and secondary production Visa Directory Server URLs and how to properly configure the MPI to automatically fall back to a secondary Directory Server if the primary Visa Directory Server is temporarily not available. Fallback **must** be configured so that no human intervention is required.

Timeout Sequencing

Verify Enrollment Requests

Merchants **must** allow at least 10 seconds for the Directory Server to send a VERes message in response to the MPI's VEReq message.

Payer Authentication Requests

The Payer Authentication Request/Response message pair has a recommended timeout value of **5** minutes, recognizing that cardholders may become distracted while completing the authentication.

Cardholder and Payment Card Data Security

Any payment card data stored by the MPI or on servers that are connected to the Internet **must** be encrypted and securely stored as described at Section 11.3, *Visa Cardholder Information Security Program (CISP)*.

For More Information

Additional information regarding mandatory and optional functionality of the MPI is contained in the document 3-D Secure: Functional Requirements – Merchant Server Plug-in.

7 Acquirer/Merchant Requirements and Best Practices

This chapter reviews additional acquirer and merchant program and transaction requirements which supplement the 3-D Secure publications and the Visa Operating Regulations. Also outlined are some recommendations for best practices to ensure a good authentication experience for customers.

7.1 Acquirer Responsibility for Merchant Participation

Participating acquirers are responsible for ensuring that participating merchants operate in accordance with the requirements in this Guide and the Visa Operating Regulations, and that such requirements are included in Merchant Agreements. Acquirers **must** ensure and/or approve the following:

- Merchants Agreements have been modified to reflect a merchant's participation in Verified by Visa.
- The issuance of a merchant client digital certificate for use in merchant authentication to the Visa Directory Server.
- Merchants and third-party commerce server providers meet the security requirements for 3-D Secure processing, including support for the Cardholder Information Security Program (CISP). CISP is based on the industry standards published in the Payment Card Industry (PCI) Data Security Standard (DSS) for protecting card and cardholder information. For further information on CISP compliance requirements, see Section 11.3, *Visa Cardholder Information Security Program*.
- Contracts with third-party commerce server providers or payment gateways **must** ensure that each merchant activated for Verified by Visa is reported to and approved by the acquirer.
- An acquirer who has contracted with a third-party service provider, or uses an Internet Payment Services Provider (IPSP), to provide Verified by Visa services to its merchants **must** complete and validate compliance with the *Visa Rules for Member Use of Non-Member Agents* document that is available through Visa Online or upon request from a Visa Representative. Acquirers may register third party agents and service providers through the Member Management application service in the *Resources* tab at Visa Online.

7.2 Merchant Authentication to Access Visa Directory Server

A merchant client digital certificate is required for participating merchants to connect to the Visa Directory Server. To support this capability, the Common Name in the merchant certificate **must** contain a Host Name (also known as a Domain Name). During the connection attempt, the Visa Directory Server will check that the client's DNS-resolvable Host Name matches the information contained in the Common Name of the merchant certificate. If the information does not match, the Directory Server will deny the connection.

7.3 **Pre-Authentication Messaging at Checkout**

Merchants **must** provide a brief message to cardholders on the checkout page after the merchant knows that the cardholder has selected a Visa card as the payment method.

The intention of the messaging is to notify the cardholder that they might next be prompted either to activate their card for Verified by Visa or, if they already participate in Verified by Visa, to provide their Verified by Visa password. The messaging is also intended to provide a further reminder and reassurance to the cardholder, beyond the presence of the Verified by Visa "Learn More" logo on the merchant's site that the merchant participates in Verified by Visa.

It is noted that some cardholders cannot be authenticated (for example, because they are not yet activated) and some will be processed as an attempted authentication. These cardholders will not be presented with a Verified by Visa password entry screen. Thus, the text **must not** refer to Verified by Visa or providing "additional security" as this message could be very confusing to these cardholders. For a pre-authentication message, merchant **must not**:

- State affirmatively that the cardholder will have a Verified by Visa experience.
- Indicate that the merchant requires the cardholder to authenticate himself or herself.
- Insert an interim page, after the cardholder clicks the "buy" button that requires the cardholder to click a "Continue" button for Verified by Visa, as this may be confusing to cardholders who are processed as an "Attempted Authentication".

Visa recommends following pre-authentication messaging which is shown in Figure 7-1.

We participate in Verified by Visa to help prevent unauthorized use of Visa cards online. When you click the [Submit or Buy] button, you may receive a Verified by Visa message from your Visa card issuer. If your card or issuer does not participate in the program, you will be returned to our secure checkout to complete your order. Please wait while the transaction is processed and do not click the 'back button' or close the browser window.

A shorter version may also be used:

The next screen you see may be payment card verification through Verified by Visa.

If the merchant is implementing Verified by Visa in conjunction with other payment card brands, and the merchant cannot determine which payment card brand is being used for the transaction, Visa recommends the following:

The next screen you see may be payment card verification through your card issuer.

The pre-authentication message is most effective and most likely to be read by cardholders when placed immediately next to the final order button.

Figure 7-1: Merchant Checkout Page with Pre-Authentication Messaging

VISA: X000-X000-X000-1234 Exp: 12/2014 Edit		Customer 123 Main City, ST Edit	Street		
Ship To:					
Customer Name 123 Main Street City, ST Zip Code			for This Shipment: and Handling:		\$19.70 \$ 2.90 \$ 1.58
(Edit)		Total fo	or This Shipment:		\$24.18
Shipping Method: Standard					
Items	Oty	Price	Gifting Option		
Description of Merchandise	1	\$24.18	Cift Wrap Not S Edit	elected	
See our <u>Return Policies</u>					
Go to the Home Page (without completing your order)			Place	Your Order)
We participate in Verified by Visa to help prevent una online. When you click the Place Your Order button message from your card issuer. If your card or issue program, you will be returned to our secure checkou	, you m er does	ay receive a ' not particip:	Verified by Visa ate in the	Verified by	
online. When you click the Place Your Order button message from your card issuer. If your card or issue	, you m er does .ttto coi	ay receive a ' not particip: nplete your	Verified by Visa ate in the order.		
online. When you click the Place Your Order button message from your card issuer. If your card or issu program, you will be returned to our secure checkou Please wait while the transaction is processed and do not	, you m er does .ttto coi	ay receive a ' not particip: nplete your	Verified by Visa ate in the order.	VISA	
online. When you click the Place Your Order button message from your card issuer. If your card or issu program, you will be returned to our secure checkou Please wait while the transaction is processed and do not	, you m er does .ttto coi	ay receive a ' not particip: nplete your	Verified by Visa ate in the order.	VISA	

7.4 Use of Framed Inline Page

The 3-D Secure Protocol requires the authentication page displays to be presented to cardholders using the full browser window in an "inline" approach. U.S. merchant 3-D Secure implementations **must** use a framed inline page for Verified by Visa. The use of a pop-up page **is not** permitted. The requirements for the use of framed inline pages are:

- The merchant **must not** display promotional messages to cardholders. It is important that cardholders have confidence in the authentication session with their card issuer.
- The frame opened for the issuer ACS to present the Verified by Visa window **must** be large enough to present the entire 390 pixel width by 400 pixel length authentication page, without scrolling, over a standard range of browser resolutions. To implement a framed inline page, merchants may place a frame at the top of the page and/or on the side of the page, as illustrated below.

Framed Inline Page with Top Frame

An inline page may have a top frame as shown in Figure 7-2.

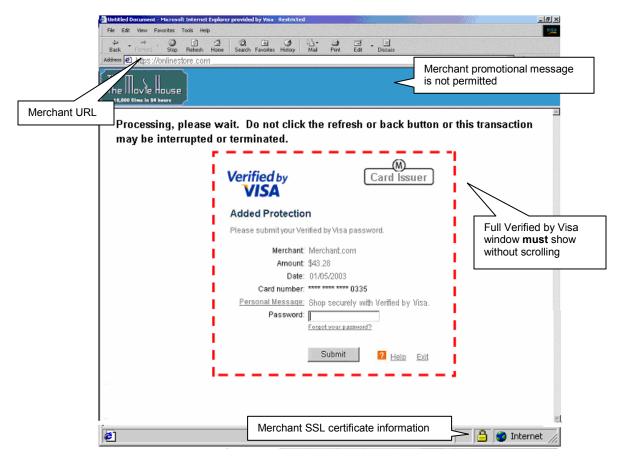
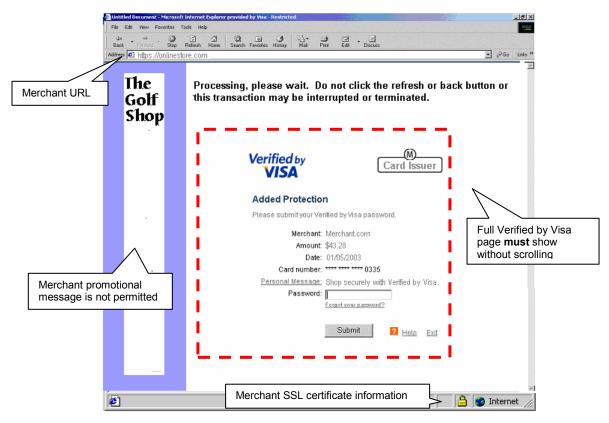


Figure 7-2: Inline Page with Top Frame

Framed Inline Page with Side Frame

An inline page may have a side frame as shown in Figure 7-3.





7.5 Text for Inline Page with a Framed Window

Merchants must provide a brief communication to customers outside of the frame for the authentication page, as shown in Figures 7-2 and 7-3 above. The recommended text is:

Processing, please wait. Do not click the refresh or back button or this transaction may be interrupted.

If the merchant elects alternate working from the recommended text, the customer communication should be free of technical jargon. Most consumers are confused by terminology that explains the technical side of Verified by Visa. Consumers may misunderstand and misinterpret messages regarding which server they are interacting with, whether they are technically at a different site, etc. Therefore, merchants should not provide text that explains, for example, "You may be taken to the secure Verified by Visa site for authentication after which you will return to our site." Merchants should keep the technology as transparent as possible to the user.

Any merchant messaging outside to the frame for the authentication page **must** avoid explicitly describing the Verified by Visa experience to the customer. The merchant is unable to determine the particular experience that a cardholder may have. For example, some cardholders will be processed as an attempted authentication and will not be presented with a Verified by Visa password entry screen. Visa usability research has shown that a simple statement, such as that recommended in this section, provides the best user experience.

Status Indicator

Visa also recommends that merchants implement a "processing" indicator with simple movement, outside of the frame for the authentication page, to provide a visual cue to customers that the purchase process is continuing in the background. Simple dots or arrows moving from left to right are sufficient for this purpose. It is important that the status indicator have some kind of simple movement. Static processing screens confuse users because they cannot tell if the system is working or frozen.

7.6 Use of Verified by Visa Merchant Symbol

Merchants **must** place the Verified by Visa "learn more" Merchant Symbol on the checkout page on which the cardholder enters their Visa card number or on another page in the checkout flow that cardholders **must** view while placing their order.



When clicked by the cardholder, the Merchant Symbol provides information on the Verified by Visa program and a link to the Verified by Visa website that provides information on Verified by Visa and allows the cardholder to activate their card in Verified by Visa. Presence of the Merchant Symbol on the checkout page notifies the cardholder that the merchant participates in Verified by Visa and alerts the cardholder to a possible interaction with the service. The *Verified by Visa Merchant Toolkit* provides information about the Merchant Symbol and standards for use. See *About This Guide--Resources and Tools* for more information.

In addition to placing the Verified by Visa Merchant Symbol on the checkout page, the following steps are recommended:

- Display the Verified by Visa "learn more" mark as early in the shopping experience as possible (e.g., merchant's home page, shopping cart).
- Wherever applicable, display the Verified by Visa "learn more" mark along with other security or better business marks (e.g., VeriSign, Thawte, BBB, etc.)
- Ensure that the Verified by Visa "learn more" mark is clearly visible and not overshadowed by other elements on the page.

When incorporating the Verified by Visa mark into the merchant website, participating merchants **must** adhere to Verified by Visa branding requirements and Visa security requirements. Merchants should ask their acquirer for information.

7.7 Activation Anytime

Visa recommends that participating merchants implement the Verified by Visa "Activate Now" symbol and link on their website, and that the "Activate Now" symbol be placed on the merchant's home page.



As described in Appendix B, *Verified by Visa Activation Anytime*, when cardholders click the "Activate Now" symbol, they are provided the opportunity to learn about Verified by Visa, and if desired, to activate their Visa card for Verified by Visa. Merchants benefit from implementing the "Activate Now" symbol by providing an opportunity for cardholders to be activated in Verified by Visa. Cardholders can leave the "Activation Anytime" landing page at any time, and return to the merchant site to continue shopping and checkout.

The Activation Anytime symbol and usage guidelines are contained in the *Verified by Visa Merchant Toolkit.* See the *About This Guide--Resources and Tools* for more information.

7.8 Failed Authentication Processing

Merchants **must not** submit for Visa authorization any transaction for which it receives a Verified by Visa failed authentication response value of **N**.

When merchants receive a Payer Authentication Response message with a failed authentication response value of \mathbf{N} , merchants **must** immediately display a message or page to communicate to the cardholder that the purchase will not be completed with the Visa card that was presented for the purchase. At the merchant's option, the cardholder may be asked to provide another form of payment. The suggested wording for the failed authentication message is:

AUTHENTICATION FAILED

Your financial institution has indicated that it could not authenticate this transaction via Verified by Visa. To protect against unauthorized use, this Visa card cannot be used to complete your purchase. You may complete the purchase by clicking here to select another form of payment.

It is recommended that merchants provide an easy, simple recovery mechanism to cardholders that fail Verified by Visa authentication. On the page on which the merchant provides the "Authentication Failure" message, the recovery mechanism may either provide an immediate opportunity for the cardholder to enter a new payment card number, including a different Visa card number, and click to try again or provide a button that, when clicked, presents a new page that allows the cardholder to easily reinitiate the purchase.

Visa also recommends that merchants provide the Verified by Visa "Learn More" link on the "Authentication Failed" page. The "Learn More" logo provides an additional opportunity to cardholders to learn about Verified by Visa.

7.9 Merchant Performance Standards

To enable participating merchants to complete sales without risk of excessively long delays in response wait time, participating merchants **must** establish minimum timeout values within the 3-D Secure Merchant Server software. The following are the Verified by Visa merchant timeout criteria:

- Verify Enrollment Request/Response. The merchant MPI software must have a timeout value of not less than 10 seconds for the Verify Enrollment Response (VERes) to be returned by the Visa Directory Server. When the timeout expires, the merchant may proceed with the transaction as a non-authenticated purchase.
- **Purchase Authentication Request/Response**. The MPI software **must** have a timeout value of not less than five minutes for the Payer Authentication Response (PARes) from the issuer ACS to allow for timing variations in the cardholder interaction, such as cardholder distraction which may delay a response.

7.10 Data Quality in VEReq and PAReq Messages

When the merchant software formats the Verify Enrollment Request (VEReq) and Payer Authentication Request (PAReq) messages to send to the issuer ACS, there are a number of data fields used for the following purposes, to:

- Identify the acquirer and merchant.
- Present transaction data to the cardholder in the authentication process.
- Conduct transaction research in the event of a cardholder dispute.

Match VisaNet and Verified by Visa Message Data Fields

Merchants **must** accurately populate the data in both VEReq and PAReq messages. Additionally, the data fields used in Verified by Visa transactions **must** match the comparable VisaNet transaction data fields, including BASE I/SMS and BASE II. Entities that host Verified by Visa on behalf of multiple merchants **must** ensure that merchant-specific data is accurate for each merchant.

Merchants **must** populate the data fields as described below.

Verify Enrollment Requests (VEReq)

- Acquirer's Bank Identification Number (Merchant.acqBIN field). This field must be the merchant's Visa acquirer's BIN. If this value is not known, merchants should ask their acquirer or merchant processor representative.
- Merchant Identifier (ID) Number (Merchant.merID field). This field **must** be the Merchant ID assigned by the acquirer to the merchant for use in Visa transactions. If this value is not known, merchants should ask their acquirer or merchant processor representative.

Payer Authentication Requests (PAReq)

Table 7-1 highlights information about requirements for a number of the data fields in the Payer Authentication Request message.

Acquirers and merchants should ensure that the data elements in Verified by Visa authentication messages match the specified data elements in VisaNet transactions.

VisaNet Field Description	3-D Secure Field Name	Comments
Acquirer's Bank Identification Number	Merchant.acqBIN	This field must match the acquirer BIN used in the Verify Enrollment Request. This field also must match the Acqurier BIN submitted in VisaNet (BASE I/SMS and BASE II) transactions.
Merchant Identifier (ID) Number	Merchant.merID	This field must match the Merchant ID used in the Verify Enrollment Request. This field also must match the Merchant ID used by the acquirer in VisaNet (BASE I/SMS and BASE II) transactions.
Merchant Name	Merchant.name	This field must contain the name of online merchant at which cardholder is making the purchase. The maximum length is 25 characters. The merchant name must match the name submitted in VisaNet (BASE I/SMS and BASE II) transactions.
Merchant Country Code	Merchant.country	This field must contain the value 840 for U.S. merchants.
Merchant URL	Merchant.url	This field must contain the fully qualified URL of the merchant site. A URL that is "fully qualified" is prefixed with the URL scheme, either "http://" or "https://".
Purchase Amount	Purchase.purchAmount	This field must contain the value of the purchase being made by the cardholder. It is a value up to 12 digits with punctuation removed, for example, an amount of \$123.45 would be 12345.
Purchase Currency	Purchase.currency	The appropriate currency code for the transaction currency between the cardholder and merchant must be used. For U.S. currency, the value is 840.
Purchase Exponent	Purchase.exponent	The minor units of currency. For U.S. dollars, the value must be 2.

 Table 7-1:
 Payer Authentication Request Message Fields

7.11 Timing between VERes and PAReq

Merchants should ensure that the MPI, upon receipt of the Verify Enrollment Response (VERes) with a value of **Y**, promptly formats and transmits the Payer Authentication Request (PAReq) to the issuer ACS URL contained in the VERes message.

When ACSs return a Verify Enrollment Response, it contains a unique Account Identifier for each transaction. To minimize the possibility of fraudulent transactions, an ACS will set a validity timer for each Account Identifier that it generates for a Verify Enrollment Response message. This timer is usually set to not exceed a period of 10 to 15 minutes because of the expectation that merchants will complete authentication processing quickly.

Payer Authentication Request messages that are received after the validity timer has expired will be returned with a failed authentication response that includes an error code. This practice reduces the likelihood that an Account Identifier can be fraudulently re-used when a Payer Authentication Response message is sent to an ACS.

7.12 Merchant Customer Support

Merchants **must** train their customer support staff on Verified by Visa so that they can respond effectively to customer inquiries. To assist merchants with the training of their internal customer support staff, Visa developed the *Verified by Visa Quick Reference for Merchant Customer Service Representatives*. Merchants should ask their acquirer or merchant processor for a copy. See the *About This Guide—Resources and Tools* section for more information.

8 Digital Certificate Use

This chapter:

- Discusses the certificate hierarchy used for Verified by Visa certificates.
- Describes the process of authenticating Verified by Visa merchants to the Visa Directory Server.
- Defines the requirements for securing 3-D Secure channels that include the merchant.

8.1 Visa Certificate Hierarchy

All Visa-issued certificates conform to X.509 standards and include a trust chain that links to the Visa 3-D Secure Root Certificate, as described in Table 8-1.

Certificate Type	Description			
Visa 3-D Secure Root Certificate	The merchant server software uses the Visa 3-D Secure Root certificate to validate the issuer signature contained in the Payer Authentication Response message. The acquirer or merchant processor obtains this certificate from Visa concurrent with the return of the signed merchant certificate, as discussed in Section 8.2. Merchant server software must be able to import and securely store the all Visa-issued certificates in the merchant's or merchant processor's certificate management key store along with the Visa 3-D Secure Root Certificate for proper operation. The Visa 3-D Secure Root certificate may be updated from time to time.			
Visa Brand Certificate	Verified by Visa certificates include an intermediate eVisa brand certificate. This certificate is returned along with the merchant client certificate.			
Visa U.S. Region Certificate	There is a second intermediate certificate issued by the U.S. Region. This certificate is referred as the USR certificate and will also be returned along with the merchant client certificate.			
Merchant Client Certificate	Visa issues client digital certificates to merchants and merchant processors participating in Verified by Visa. The merchant client certificate is used to authenticate the merchant to the Visa Directory Server. The merchant's or merchant processor's Visa acquirer must submit the certificate request to Visa on behalf of its merchants and/or merchant processors.			

Acquirers will find the forms to request merchant certificates through Visa Online. Click on the *Products and Services* tab, then, click on the "Verified by Visa" link. On the left side, click "For Acquirers;" the certificate request form is in the list of "Useful Acquirer and Merchant Tools."

8.2 Merchant Authentication

Merchant authentication is the process by which the Visa Directory Server identifies a specific merchant and determines whether the merchant is authorized to participate in the Verified by Visa program. The merchant is authenticated each time the Merchant Server Plug-in (MPI) transmits a 3-D Secure message to the Visa Directory Server.

If the merchant fails authentication, the Visa Directory Server returns an error message as described in Table 4-2, *Verify Enrollment Response Values*. In this case, the merchant is not permitted to submit an authorization request for the transaction.

Using Client Certificate Merchant Authentication

U.S. Verified by Visa merchants are required to be authenticated to the Visa Directory Server by use of a Visa-rooted client digital certificate that the merchant presents to the Visa Directory when attempting a connection. The merchant certificate is required by the Directory Server before allowing a connection to process Verify Enrollment messages.

Visa **must** receive authorization from the merchant's acquirer before a client certificate signed by the Visa 3-D Secure Root Certificate will be processed. Merchants should contact their acquirer or merchant processor for information about 3-D Secure client certificates. Merchants that operate their own commerce servers and connect directly to the Directory Server **must** obtain a Visa-signed client certificate.

Acquirers, at their discretion, may contract with a third-party processor that hosts multiple merchants signed by that acquirer. The acquirer may approve the issuance of a Visa-signed client certificate to the processor for all of the acquirer's merchants. Alternatively, the acquirer may require the processor to support client certificates for each merchant processed for that acquirer.

Note:

Individual client certificates must be used for each merchant whose business requires a Merchant Category Code (MCC) within the High Risk Sponsored Merchant program. Additionally, a separate Visa client certificate must be used for each high risk Internet Payment Service Provider (IPSP).

Third-Party Service Providers, High Risk Merchants, and Internet Payment Service Providers must be registered by their acquirer using the Member Management application service via the "Resources" tab at Visa Online

U.S. Verified by Visa merchants are authenticated via merchant certificates, as follows:

- The MPI (or the merchant server) generates a public/private key pair and stores it securely.
- The MPI (or the merchant server) generates a certificate request using the key pair it generated.
- Using a procedure specified by the acquirer, the MPI or merchant server provides the certificate request to the Visa Certificate Authority specified by the acquirer.
- The Visa Certificate Authority returns a certificate response including the Visa 3-D Secure Root, Visa Brand and merchant client certificates.

- The MPI (or the merchant server) processes the certificate response and loads the certificates in a secure manner.
- During each instance of 3-D Secure transaction processing, the MPI presents the certificate and the Visa Directory Server validates it.

8.3 Transport Security

All 3-D Secure messages depend upon transport security to provide confidentiality. Before sending a data message between 3-D Secure components, the channel over which the message is transmitted **must** be secured through the establishment of an SSL session using a TLS/SSL Server Certificate. Typically, merchants with existing websites will have obtained such certificates during the ordinary course of business. If not, the operator of the MPI **must** obtain a TLS/SSL Server Certificate from a commercial certificate authority.

The merchant participates in two channels during 3-D Secure processing. These channels, and the component responsibility for securing each channel, are described below.

Cardholder to Merchant

The channel between the cardholder and the merchant is used to transmit:

- The cardholder's payment information to the merchant.
- The Payer Authentication Request message from the MPI through the cardholder device to the Visa Transaction Routing Service and ACS.
- The Payer Authentication Response message from the ACS and Visa Transaction Routing Service through the cardholder device to the MPI.

The merchant's commerce server **must** secure this channel with an SSL session initiated using its TLS/SSL Server Certificate.

Merchant to Visa Directory Server

After validating the Merchant Certificate, Visa Directory Server secures the channel with the Merchant Server Plug-in and transmits:

VEReq / VERes Message Pair

- The MPI's query about the availability of 3-D Secure processing for a specific cardholder.
- The response (from the Visa Directory Server or forwarded by the Visa Directory Server from the ACS) indicating whether 3-D Secure processing is available for the cardholder. If it is, the response includes the URL to which the MPI will direct requests for cardholder payment authentication.

The Visa Directory Server will secure this channel with an SSL session using its TLS/SSL Server Certificate.

9 MPI Implementation Options

This chapter reviews some alternatives for implementing Merchant Server Plug-in (MPI) functionality to enable merchant participation in Verified by Visa.

Merchants that elect to participate in Verified by Visa will want to assess their business requirements, technological capabilities, and current operating environment to determine what approach they should pursue. The MPI can be located at the merchant location, at the acquirer or processor site, or at the merchant service provider.

Among the implementation options available to merchants are the following:

- Purchase components from a technology provider and integrate into an existing system.
- Purchase a complete storefront package from a technology provider.
- Develop MPI software using internal or contracted resources. The product developed **must** adhere to the requirements described in the documents *3-D Secure Protocol Specification— Core Functions* and *3-D Secure: Functional Requirements—Merchant Server Plug-in.*
- Obtain MPI hosted processing services from a third party payment services provider.
- Subscribe to the full complement of electronic commerce merchant services provided by a third party, such as a mall operator.
- Obtain MPI processing, if offered, from the merchant's Visa acquirer.

Note:

Regardless of the MPI implementation option selected, Visa requires that merchants adhere to the requirements described in this Guide.

Copies of the 3-D Secure Protocol Specification and the 3-D Secure Functional Requirements --Merchant Server Plug-In are available from Visa after completion of a license agreement. To request a copy of the license agreement, send an email to <u>3DCompliance@visa.com</u>.

9.1 Buy Options for MPI Software

Packaged Software Option

MPI software can be purchased and implemented without extensive modification to a merchant's existing commerce server. The MPI can either scan each request from a consumer's device to detect and intercept a "Buy" page, or be provided the required "Buy" page data by the merchant commerce server. This approach provides for a loose coupling between the merchant commerce server code and the MPI software, and minimizes code changes required to the merchant application or the commerce server.

3-D Secure compliant MPI packaged software is available from software developers for most common Internet platforms, such as Sun/Solaris, Microsoft/Windows, and Linux. For information on available software solutions, visit the following link:

https://partnernetwork.visa.com/vpn/global/category.do?categoryId=85&documentId=117&userRe gion=1

A simple implementation may take as little as six weeks to integrate, test, and certify. The degree of integration, customization, and vendor support a merchant chooses will affect the integration time and cost. Costs for the MPI solution may vary (up-front fees, per transaction, etc.), so merchants are recommended to investigate several vendors about pricing and options.

This approach can provide an attractive solution for small to medium-size merchants with limited resources in terms of time, software engineering skills, and finances.

Software Development Kit (SDK)

A Software Development Kit (SDK) provides a set of callable interface options for each step required of the merchant in the Verified by Visa authentication process. A merchant with appropriate engineering resources can use an SDK to integrate Verified by Visa into its existing merchant commerce application. This approach provides the merchant with a high degree of control over the execution and monitoring of each step of the MPI implementation, and can enable a high degree of functional MPI efficiency.

The SDK typically needs to support the following services:

- Creating VEReq, PAReq, and error messages (3-D Secure messages are described in Chapter 4, *3-D Secure Messages*).
- Processing VERes and PARes error messages.
- Validating the signature on PARes messages.
- Communicating with the Visa Directory Server (may be optional; can be provided by most commerce server platforms).

An SDK can provide a good solution for medium size and large merchants, merchants with complex processing requirements, or merchants that require a high degree of operational control.

9.2 Hosted MPI Options

Internet Payment Service Provider

Numerous Internet service providers offer services allowing customers to set up and run a website. Along with utilities to simplify the set up and administration of the website, these service providers frequently partner with one or more payment service providers to offer support for the processing of online payments. In this model, the service provider develops and deploys software that is integrated with one or more Internet payment service provider or traditional acquirer processing systems.

Internet Payment Gateway Service Provider

An Internet payment gateway provides a way for Internet merchants to route an online payment transaction from the merchant's website to a legacy transaction processing system offered by a traditional brick-and-mortar payment processor. The payment gateway provides the bridge between the Internet systems of the merchant and the legacy systems of the payment processor.

Internet gateway providers often partner with one or more payment processors to offer support for online payments processing, as well as utilities to simplify the set up and administration of online payments. In this model, the payment gateway provider has developed and deployed software that is integrated with one or more legacy payment processing systems. As with the Internet payment service provider option, when an Internet payment gateway provider's payment platform is 3-D Secure-enabled, every merchant using that platform has the capability to offer Verified by Visa.

Acquirer MPI Service

Acquirers, particularly those currently operating front-end point-of-sale systems for their merchants, may elect to enhance their traditional authorization and data capture transaction processing service offerings by adding support for MPI functionality. By incorporating Verified by Visa into its front-end systems, an acquirer can provide its merchants with an additional service and enable them to participate in the Verified by Visa program.

Acquirers that desire to develop MPI software for participation by their merchants in Verified by Visa should obtain the following documents. (See *About This Guide—Resources and Tools* for more information.)

- 3-D Secure: Protocol Specification—Core Functions
- 3-D Secure: Functional Requirements—Merchant Server Plug-in

Prior to moving the customized MPI software into its production environment, the acquirer **must** successfully complete testing to prove compliance with Visa International's requirements. Details of the required testing are defined in:

- 3-D Secure: Compliance Testing Facility—Policies and Procedures
- Chapter 10, Implementation Considerations

9.3 Custom Software Development

Merchants who want to develop their own custom software for 3-D Secure should complete the Visa license agreement and obtain the following documents. (See *About This Guide—Resources and Tools* for more information.)

- 3-D Secure: Protocol Specification—Core Functions
- 3-D Secure: Functional Requirements—Merchant Server Plug-in

Development of the MPI does not require the use of any proprietary algorithms or software. Many of the software components required to develop a custom 3-D Secure implementation can be downloaded from the Internet (for example, from www.openssl.org) free of charge. If the merchant has adequate software engineering resources, the development of customized software is a feasible option to pursue.

After development, but prior to moving the customized MPI software into its production environment, the merchant will be required to successfully complete testing to prove compliance with Visa International's requirements. Details of the required testing are defined in:

- 3-D Secure: Compliance Testing Facility—Policies and Procedures
- Chapter 10, Implementation Considerations

Custom software development of the MPI may be the ideal solution for large merchants possessing adequate project management and engineering resources to plan, analyze, and implement the 3-D Secure Protocol.

10 Implementation Considerations

This section discusses implementation considerations in general. Appendix A provides an example of planning and implementation steps for merchants that purchase a Merchant Server Plug-in to integrate with the web storefront software at their location.

10.1 Participation, Decision, and Project Team

Information Phase

Merchants gather information about Verified by Visa, including:

- Program information, in addition to that available in this implementation guide, is available at http://usa.visa.com/merchants/risk_management/vbv.html
- Software and system requirements information may be available from acquirers or acquiring
 processors. Additionally, *About This Guide—Resources and Tools* lists sources of technical
 publications.
- Information on technology solutions and technology providers may be available from acquirers or acquiring processors.
- A list of vendors offering Verified by Visa compliant MPI products is available at:

https://partnernetwork.visa.com/vpn/global/category.do?categoryId=85&documentId=117&userRe gion=1

Upon completion of the information phase, a merchant will have a good understanding of the Verified by Visa program and what is required to participate.

Participation Evaluation

Using the information gathered about Verified by Visa, a merchant reviews the program and requirements, and then determines whether to participate in the Verified by Visa program. If the merchant decides to participate, the merchant should complete the necessary contractual agreements with its acquirer or merchant processor and establish a target live date.

Technology Solutions Evaluation

The merchant reviews the various software solutions available and determines the best fit for its technology environment. This may involve both documentation reviews and specific technology provider presentations. Detailed discussions of the merchant environment and technology solutions may require non-disclosure agreements between the parties to protect confidentiality.

Once the merchant has completed its assessments, it selects a vendor and solution, and completes the appropriate contractual agreements. Throughout this process, merchants should ensure the participation of its acquirer or acquiring processor.

Establish Implementation Team

A successful implementation project starts with the identification of the key project areas and team members. This team comprises representatives from the merchant's technical and operations groups, along with technology provider and acquirer personnel.

Marketing and customer support areas should also be included in the overall plan to ensure good organizational communication about the project status. The implementation team will be responsible for the timely completion of implementation activities.

Create Project Plan

The implementation team identifies a project manager and begins creation of a detailed project plan. The plan should include checkpoints, key deliverables, responsible parties, and milestone tasks such as:

- Merchant internal software development (if needed)
- Installation of software in merchant development environment
- Merchant configuration, including response handling, system monitoring, field handoff to authorization system, and data storage.
- Quality assurance testing
- Production rollout, including a phased rollout, if appropriate

Execute Project Plan

The team executes the plan as detailed, ensuring all tasks are completed as planned.

10.2 Development Phase

Develop Internal Software

Depending on the software solution selected, the merchant may need to develop specific code to deal with software calls and responses.

Install Software into Development Environment

The merchant (or technology integrator) installs the merchant server software into the development environment and completes any necessary configuration adjustments, including response handling, system monitoring, integration with authorization system, and data storage.

The merchant's Visa acquirer or merchant processor will provide information about the Verified by Visa Directory Server URL to be used when installing the merchant server software.

10.3 Testing Phase

After the merchant server software has been installed in the merchant's development environment, the merchant performs the tests required to prepare the software for implementation.

Merchant Performs Unit and System Testing

The merchant performs unit testing to ensure that the software was successfully installed. During unit testing, the merchant software communicates with test servers. Testing **must** be done to confirm that the software is able to pass information to the appropriate servers and send information from the servers to the merchant. Visa provides a free testing site, https://dropit.3dsecure.net/PIT, which all merchants are highly encouraged to use. See Section 10.4, *Requirements for Pre-Production Readiness via the PIT* for information about PIT testing.

Additional Internal Testing: After unit testing has been successfully completed, the merchant may perform additional testing according to internal requirements and procedures. Additional testing may include regression, stress, and QA testing. After testing is completed, the merchant informs its acquirer that it is ready to establish a production link.

Migration to Production

The merchant determines a production date and notifies its acquirer to coordinate and plan certification testing. The acquirer or merchant processor provides the URL and port numbers of the production servers for the Verified by Visa program. The merchant makes code changes to enable the software to point to the production servers and performs testing to make sure that communication with the servers is successful. The software is now ready for production.

10.4 Requirements for Pre-Production Readiness via Product Integration Testing (PIT)

Visa has implemented a 3-D Secure Product Integration Testing (PIT) facility. The goal of PIT facility testing is to ensure that new Access Control Server (ACS) and Merchant Plug-in (MPI) implementations of the 3-D Secure program meet technical and business requirements, and will provide a consistent user experience for Visa cardholders, before going live in production.

PIT Certification Procedures

Visa requires that new 3-D Secure implementations in the U.S. successfully pass all PIT test cases before production digital certificates for 3-D Secure will be fulfilled and before implementations go live in production. The procedures are as follows:

- Ensure that the implementation is production-ready.
- Enroll in the PIT. The PIT URL is: <u>https://dropit.3dsecure.net/PIT/</u>.
- To connect to the PIT, request (using the PIT online facility) and install the PIT test certificates and perform all PIT test cases until all have been successfully completed per the PIT User Guide and Test Plan documentation.

Auditing of PIT Results

Visa may elect at any time to audit PIT test case results. If Visa determines that all test cases were not passed by the 3-D Secure implementation, and/or that the implementation does not conform to Visa product rules (as described in Chapter 7, *Acquirer/Merchant Requirements and Best Practices*). Visa will require re-certification via the PIT and may, at its sole discretion, require that 3-D Secure production processing cease until the implementation is successfully certified and complies with product rules.

The test cases in the PIT will evolve over time. Visa reserves the right to add, delete, or modify the test scripts at any time. Visa also reserves the right, at its sole discretion, to require 3-D Secure implementations to re-test via the PIT and successfully complete one or more additional test cases.

MPI Requirements

The following new implementations **must** certify via the PIT:

- Merchant-hosted MPI.
- Processor-hosted MPI.
- Processor does not host merchant's commerce server: Each merchant must be certified individually to ensure that it has correctly integrated 3-D Secure processing into its commerce server.
- Processor hosts commerce server: At a minimum, the processor must certify its first merchant implementation via the PIT. However, if the processor centrally hosts both the MPI

and the commerce server for its merchants (such that additional merchant implementations of 3-D Secure do not require additional integration), additional certification via the PIT is strongly recommended but not required.

Re-certification Requirements:

Re-certification is required in the event of any of the following.

Switch to New MPI Software

If an existing MPI implementation changes to a different software package, either from a new vendor or to an in-house-developed package, the implementation **must** successfully complete PIT testing.

Change in MPI Processor

If a merchant switches to a new MPI processor, or moves from a processor to an in-house implementation, the new implementation is subject to the PIT certification requirements as stated above.

Software Updates

If a new version of existing MPI software is implemented that contains significant changes over prior versions, testing is needed to ensure that the revised implementation can successfully complete PIT testing.

Test 3-D Secure Software Installation

The following tests are recommended:

- Perform end-to-end testing, using a variety of browsers, to ensure that the software was correctly installed.
- Test software responses with various transaction scenarios, both positive and negative, including incorrect password entries that result in a failed authentication response.
- Confirm that an ECI value of **5** is passed when transactions are successfully authenticated and an ECI value of **6** is passed when the merchant attempts to authenticate but the cardholder does not participate in Verified by Visa. In both cases, if a CAVV is received in the authentication response, confirm that CAVV data is forwarded in the BASE I authorization request message. When appropriate, coordinate testing with the acquirer, gateway, or merchant processor to confirm that the ECI values of **5** and **6** are being handled correctly.

After testing is complete and the software is functioning correctly, the merchant notifies its acquirer or acquiring processor.

10.5 Pre-Production Implementation Checklist

Before coming live in production, participating merchants **must** ensure its implementation meets all Verified by Visa requirements. Merchants **must** successfully complete all of the items on the Pre-Production Implementation Checklist, provided in Table 10-1 below, prior to deploying Verified by Visa into production. To ensure continued compliance with Verified by Visa requirements, Visa strongly recommends that merchants review their adherence to the items on the checklist should the merchant make subsequent, substantial changes to its implementation of Verified by Visa or to its checkout process.

Item	Description/Reference	Y
Acquirer Registers Service Providers using Member Management Application Service at Visa Online	Required: An acquirer who has contracted with a third-party service provider, or uses an Internet Payment Services Provider (IPSP), to provide VbV services to its merchants must register the service provider via the Member Management application service. Visit Visa Online and click on the <i>Resources</i> tab.	
CISP Compliance	Required: Website is CISP-compliant. If the MPI will be hosted by a third party or an Internet Payment Service Provider, a third-party CISP audit may be required, and sufficient lead time should be allocated for completion of this task. See Section 7.1, Acquirer Responsibility for Merchant Participation and Section 11.3, Visa Cardholder Information Security Program (CISP).	
Digital Certificate	Required: Acquirer approval has been obtained for the merchant to initiate PIT Testing and request production certificates. See <i>About This Guide—Resources and Tools</i> and Chapter 8, <i>Digital Certificate Use</i> .	
Request and PIT Testing Preparation	Acquirers will find the forms to request merchant certificates via Visa Online. Click on the <i>Products and Services</i> tab, then, click on the "Verified by Visa" link. On the left side, click "For Acquirers." The certificate request form is in the list of "Useful Acquirer and Merchant Tools."	
Pre-Authentication Messaging Required: Merchant provides messaging, that follows Visa guidelines, to the cardholder prior to the initiation of VbV processing. See Section 7.3, <i>Pre-Authentication Messaging at Checkout</i> .		
Inline Presentation	Required: VbV implementation is a framed inline page; see Section 7.4, Use of Framed Inline Page and Section 7.5, Text for Inline Page with a Framed Window.	
3-D Secure Timeout Values Required: Merchant has set appropriate timeout values for receipt of VERes and PARes messages. See Section 7.9, <i>Merchant Performance</i> <i>Standards</i> and Section 7.11, <i>Timing between VERes and PARes</i> .		
Authentication Failure Messaging	Required: Verified by Visa-specific messaging for authentication failures that follows Visa guidelines has been implemented.	
Authentication Failure Messaging	Best Practices: The cardholder is provided a smooth method for reinitiating the transaction using (the same or) a different payment card, and the Verified by Visa "learn more" logo is provided on the "Failed Authentication" page. See Section 7.8, Failed Authentication Processing.	

 Table 10-1:
 Required Merchant Implementation Checklist

Table is continued on the next page.

Item	Description/Reference	V
VbV Merchant Symbol	Required: VbV Merchant Symbol is installed on the checkout page. See Section 7.6, <i>Use of Verified by Visa Merchant Symbol</i> .	
"Activate Now" Link Best Practice: "Activate Now" button/link is installed correctly on at least one merchant page. See Section 7.7, <i>Activation Anytime</i> .		
VbV Message Values	Required: Data is populated accurately in all 3-D Secure message fields. See Section 7.10, <i>Data Quality in VEReq and PAReq Messages</i> .	
Monitoring	Required: MPI is integrated into merchant's production monitoring processes. See Section 6.2, <i>Additional MPI Functional Requirements: Monitoring</i> .	
Customer Support Training	Required: Customer support staff have received VbV training. See Section 7.12, <i>Merchant Customer Support</i> .	
Authorization Processing	Required: Merchant correctly populates VbV data in the authorization message. See Chapter 5, <i>Authorization Processing</i> .	
PIT Testing	Required: PIT testing has been successfully completed. See <i>About This Guide–Resources and Tools</i> , for information about how to obtain the Product Integration Testing (PIT) Facility documents.	
Digital Certificate Installed	Required: After successful completion of PIT testing, the acquirer can obtain the requested production client certificate. The merchant installs and tests the production certificates in preparation for launch.	

Table 10-1:	Required Merchant Implementation Checklist (Continued)
	roquired merchant implementation enconnet (continued)

10.6 Merchant MPI System Resiliency

Merchants and third-party service providers that operate MPI capabilities are strongly recommended to adopt system resiliency plans for their Verified by Visa operations. These plans may include the components listed below.

- Implement adequate controls to reduce the risks and exposures of an interruption to critical or significant business processes and services due to a major disaster or failure. This includes a Business Impacts Assessment to create an inventory of enterprise recovery plans in the event of a service interruption.
- System redundancy of critical production components; ideally located in physically separate data centers.
- Failover processing logic to ensure connectivity with an alternative Visa Directory Server (DS) in the event connection with the initial Visa DS connection is unavailable.
- Establish data center disaster recovery plans that are tested multiple times a year.
- Ensure data files are synched (data file replication) between alternate systems regularly and frequently.
- Establish monitoring of physical equipment (servers, switches, etc.) and software with alerts generated if operating components do not support established parameters.
- Establish monitoring of e-commerce server availability via multiple Internet locations.
- Ensure back-up across all servers and store back-up media at an off-site location.
- Develop and maintain supporting documentation with procedures for crisis management, emergency operations, and work area recovery responses. Ensure that tests of disaster recovery plans include incident command documentation.

11 Risk Management

It is recommended that merchants define and maintain a risk management function for all electronic commerce initiatives, including support for Verified by Visa. Merchants **must** maintain their existing electronic commerce risk management functions during and after the implementation of Verified by Visa. These functions should include:

- Risk management procedures already in place for Internet and electronic commerce activities.
- Existing policies and procedures for sensitive cardholder and payment card data storage, known as the Visa Cardholder Information Security Program or CISP.
- Understanding fraud and chargeback risks and liabilities.
- Procedures for tracking and monitoring fraud allegations and losses.

Electronic commerce transactions have a higher level of cardholder disputes than card-present transactions (i.e., retail purchases in the physical world) and other card-not-present transactions (e.g., mail order and telephone order). Disputes related to unauthorized use or "I didn't make the purchase" allegations account for over three-quarters of all disputes for electronic commerce transactions. The back office expense and losses associated with these disputes adversely affect the profitability of merchants and other parties involved in payment processing.

Risk management considerations play a vital role in how a merchant implements and manages a Verified by Visa program. Key areas that merchants should consider include:

- Website Content Customer relationships can be strengthened by merchants using their website not only as a marketing tool to increase revenue, but also a risk management tool to avoid customer disputes. This includes privacy, delivery, refund, and credit policies, as well as customer service contact information (e.g., toll free number, email address, etc.).
- Website Tracking and Analysis By tracking and analyzing website activity, merchants can learn more about Internet visitors and identify shopping patterns with high levels of risk exposure.
- Data Security If merchants need to store sensitive cardholder information (e.g., account numbers, expiration dates, identity numbers, name and address, etc.), they **must** ensure that any sensitive information is stored in a secure manner (e.g., encrypted, scrambled, or stored offline with appropriate access controls in place) in accordance with the Visa Cardholder Information Security Program requirements; see Section 11.3 for more information.

See Appendix C, *Best Practices: Fraud Screening*, for best practice recommendations for screening for fraud transactions.

11.1 Related Security Programs

Other programs and Visa documentation that promote data security complement the Verified by Visa program and best practices.

Visa provides risk management documentation to help merchants to identify risk exposures specific to the Internet and to implement solutions for secure commerce. A copy of *Visa E-Commerce Merchants' Guide to Risk Management* is available on Visa.com. See *About This Guide*—*Resources and Tools* for more information.

11.2 Excessive Chargebacks and/or Fraud

U.S. merchants with excessive chargebacks or excessive fraud may be identified for the following programs:

U.S. Programs

- U.S. Merchant Chargeback Monitoring Program (MCMP)
- Risk Identification Service (RIS) Online

Any merchants identified for these programs are not permitted to submit Verified by Visa transactions as authenticated (ECI **5**) or attempted authentication (ECI **6**) during the time that the merchant is in the Program and for a period of 4 additional months thereafter. If a merchant participates in Verified by Visa, transactions **must** be submitted with an ECI **7**.

International Programs

Global Merchant Chargeback Monitoring Program (GMCMP)

Any merchants identified for this program are not permitted to submit Verified by Visa transactions as attempted authentication (ECI **6**) during the time that the merchant is in the Program and for a period of 3 additional months thereafter. If a merchant participates in Verified by Visa, attempted authentication transactions **must** be submitted with an ECI **7**.

Global Merchant Fraud Performance (GMFP)

Any merchants identified for this program has generated an excessive level of reported fraudulent transactions. Issuers are permitted to charge back identified transactions using Reason Code 93.

Merchants should contact their acquirer or merchant processor for more information regarding the criteria for these programs.

Important Notice to Acquirers and Merchants:

Participation in Verified by Visa can be a valuable fraud management tool. Merchants identified for any of the programs above are encouraged to implement support for Verified by Visa as one of the security and risk management tools they employ.

It should be understood that even with Verified by Visa participation, an issuer will investigate cardholder allegations of fraud and if the issuer determines that fraud occurred, the fraud transactions are required to be reported to Visa even though Verified by Visa rules may not permit the issuer to initiate chargebacks.

11.3 Visa Cardholder Information Security Program (CISP)

All merchants **must** implement support for the Visa Cardholder Information Security Program (CISP). This program requires use of the Payment Card Industry (PCI) Data Security Standard (DSS), a proven methodology that enables users to achieve an immediate and significant improvement in the system-wide level of security. The program applies to any entity that stores or processes Visa card and cardholder account data. All such entities will be required to store this information in a safe and secure manner, and a set of Security Standards has been put in place in order to help achieve a secured environment. For more information, visit:

http://usa.visa.com/merchants/risk_management/cisp.html

11.4 Verified by Visa Global Performance Standards

Verified by Visa was designed to act in conjunction with other fraud mitigation tools. Acquirers/merchants are not permitted to rely exclusively on Verified by Visa for fraud and risk mitigation. Merchants **must** use an adequate combination of fraud screening and risk mitigation tools available to ensure that fraud is managed to the lowest possible level.

Visa has identified Merchant Transaction Quality standards that are described in Appendix D. *VbV Global Performance Enhancement Program*. The standards set forth levels of excessive chargebacks which merchants **must not** exceed.

12 Dispute Resolution

12.1 Applicable Operating Regulations

The Visa Operating Regulations specify that issuers may not charge back electronic commerce transactions for certain chargeback reason codes under the following conditions:

- The cardholder indicates that he/she does not recognize or did not authorize the purchase, and
- The transaction involved either a Verified by Visa authentication or attempted authentication.

If a disputed electronic commerce transaction would potentially qualify to be charged back under one of the reason codes below, additional research may be required.

Chargeback Reason Codes:

- Reason Code 75 Cardholder Does Not Recognize Transaction
- Reason Code 83 Fraudulent Transaction Card-Absent Environment

Acquirers should consult the *Verified by Visa Operations and Dispute Resolution Guide* for additional information about dispute resolution processing. A copy can be accessed through Visa Online.

Exceptions to Chargeback Processing Rules for Attempted Authentications

There are four exceptions to the rules for attempted authentications. If a purchase transaction is conducted with one of the following and proof of attempted authentication is returned, issuers may follow procedures for standard (non-authenticated) electronic commerce purchases if disputed by the cardholder:

- A Visa Commercial card product (Business, Corporate, or Purchasing cards),
- An anonymous Prepaid card, such as a Gift card,
- A Visa-designated new channel device, or
- A merchant identified in monitoring programs for excessive chargebacks or fraud; see Section 11.2, *Excessive Chargebacks and/or Fraud*, for more information.

If the cardholder using a Visa Commercial card, anonymous Prepaid card, or mobile device is authenticated by an issuer using Verified by Visa (an ECI 5 transaction), the Verified by Visa dispute resolution procedures for authenticated transactions apply and the issuer may not submit a chargeback for the two reason codes above.

Exceptions to Chargeback Processing Rules for Both Authenticated and Attempted Authentication Transactions from U.S. Merchants

While Verified by Visa is designed to provide additional security to merchants, certain types of transactions have proved to be unusually vulnerable to fraud. As a result of the disproportionate fraud risk being introduced by such transactions, chargeback protection has been eliminated for U.S. merchants in the four merchant category codes listed below for Verified by Visa authentications and attempted authentications when conducted by U.S. cardholders for merchants in the following MCCs:

- Wire Transfer/Money Order (MCC 4829)
- Direct Marketing-Inbound Teleservices (MCC 5967)
- Non-Financial Institution-Foreign Currency, Money Order (not Wire Transfer), Travelers' Cheques (MCC 6051)
- Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting and Wagers at Race Tracks (MCC 7995)

Thus, U.S. issuers and issuer processors are eligible to submit chargebacks for Reason Code 75 (Cardholder Does Not Recognize Transaction) and Reason Code 83 (Fraudulent Transaction– Card-Absent Environment) for merchants in the above MCCs. The acquirer may not represent these chargebacks even if the transaction was authenticated or an attempted authentication.

Important Notice:

The removal of chargeback protection in these four MCCs does not apply to international Verified by Visa authenticated and attempted authentication transactions.

Non-U.S. issuers will not be able to submit chargebacks for properly processed authenticated or attempted authentication transactions.

U.S. issuers will not be able to submit chargebacks for non-U.S. acquired transactions that are properly processed as authenticated or attempted authentications where the acquirer included the correct ECI and CAVV.

12.2 Merchant Transaction Records

To assist in the investigation of disputes associated with transactions that were processed using 3-D Secure, the merchant **must** save a copy of each Payer Authentication Response (PARes) message received from an issuer ACS, as well as the associated PAN,20 and **must** be prepared to provide this data on request. The information **must** be retained for a minimum of six months (and a maximum of two years).

Note:

The merchant server software cannot rely on a full PAN value to be returned in the PARes, as any issuer ACS that is using version of the protocol is required to mask the PAN in the PARes message. The most that is guaranteed to be returned is the last four digits of the PAN that was submitted in the Verify Enrollment (VEReq) message.

12.3 Dispute Processing – Acquirer Quick Reference

Table 12-1 provides a recap of the data field important for acquirer use in dispute processing for transactions where the cardholder was authenticated.

Author Request I	rization Message	Authorization Response Message	Settlement Transa	-	Chargeback Processing		on Response (PA r ACS to Mercha	
Electronic Commerce Indicator (ECI)	CAVV Field Populated	CAVV Results Code	Electronic Commerce Indicator (ECI)	Chargeback Rights Indicator (CRI)	Chargeback Processed or Blocked	Authentication Response Value	Electronic Commerce Indicator (ECI)	CAVV Field Populated
1. Cardholde	1. Cardholder Authentication by Issuer ACS and U.S. Acquirer/Merchant Provide Valid Fields in Authorization and Settlement							
5	Yes Note: CAVV is required for ECI 5 trans.	Any CAVV Results Code value is valid except Blank , 0 , B	5	12 = T&E Tran or 13 = Retail Tran Int'I Note: CRIs are not assigned when issuer is not U.S.	RC 75 and RC 83 Blocked	Y = Cardholder Authenticated	5 = Cardholder Authenticated	Yes
2. Cardholde Settlement	er Authentica	ation by Issuer ACS	, but U.S. Acquir	er/Merchant D	D NOT Provide	Valid Fields in <i>I</i>	Authorization and	I
5	CAVV could be populated or not	CAVV Results Code value is one of the following: Blank = No CAVV 0 = Invalid CAVV B = CAVV, but no VbV chargeback protection	7 U.S. Note: Because the CAVV was not valid, acquirer is required to submit an ECI 7 in BASE II Int'I Note: If Issuer Country Code \neq 840 and issuer is not a VbV participant, BASE II will downgrade to ECI 7	Not Applicable	RC 75 and RC 83 Not Blocked	Results Code va Authorization Re indicate whether submitted a valid transaction. See and Dispute Res The acquirer ma provide a copy of	aded to determine alue returned in the esponse. This valu the merchant/acc d CAVV for an aut <i>verified by Visa</i> (solution Guide, Ch ay need to ask the of PARes message on Status, ECI and	e will juirer henticated <i>Operations</i> apter 6. merchant to e, including
Note to Acquirers: Properly processed Verified by Visa transactions where the cardholder was authenticated will not be subject to chargebacks for Reason Code 75 or 83. If, however, there were processing issues as indicated by an invalid CAVV Results Code value in the VisaNet Authorization Response, issuers will be permitted to charge back disputed transactions. Acquirers should start dispute research by reviewing the CAVV Results Code value returned in the VisaNet Authorization Response. Acquirers may need to request documentation from the merchant to determine if there was a CAVV in the Authorization Request and if the same value was returned in the PARes. If the merchant provides documentation that a valid PARes with an Authentication Confirmation was received, the acquirer can submit a Representment along with supporting documentation.								

Table 12-1: Dispute Processing Summary for U.S. Acquirers – Authenticated Transactions

If an acquirer receives a Pre-Compliance request from a non-U.S. issuer to dispute a Verified by Visa transaction and research determines all transaction requirements above were met, the acquirer may respond that VbV authenticated transactions are not eligible to be charged back. Documentation includes the PARes transaction with the Authentication Results Value, ECI and CAVV if these data elements were included in the PARes.

Table 12-2 provides a recap of data fields important for acquirer use in dispute processing for transactions where the merchant attempted to authenticate the cardholder.

Table 12-2: Dispute Processing Summary for U.S. Acquirers – Attempted Authentications

Authorizatio Mess		Authorization Response Message	Settlement BASE II Transaction	Chargeb	ack Processing	Authentication Issuer	Response (PA ACS to Mercha	
Electronic Commerce Indicator (ECI)	CAVV Field Populated	CAVV Results Code	Electronic Commerce Indicator (ECI)	Chargeback Rights Indicator (CRI)	Chargeback Processed or Blocked	Authentication Response Value	Electronic Commerce Indicator (ECI)	CAVV Field Populated
3. Attempted	Authenticatio	on by U.S. Merchant	and U.S. Merch	ant/Acquirer P	ovided Valid Fields in	Authorization an	d Settlement	
6	Yes	Any CAVV Results Code value is valid except Blank, 0, B	6	12 = T&E Trans or 13 = Retail Trans. Int'l Note: CRIs are not assigned when issuer is not U.S.	RC 75 and RC 83 Blocked Int'I Note: For non- U.S. issuers that participate in Attempts, RC 83 will not be blocked so U.S. acquirers will need to Represent with documentation	A = Attempt	6	Yes
4. Attempted	Authenticatio	on by Merchant, but	Merchant/Acqui	rer DID NOT P	ovide Valid Fields in A	Authorization and	/or Settlement	
6	Yes, unless CAVV Result Code value is Blank	CAVV Results Code value is one of the following: Blank = No CAVV 0 = Invalid CAVV B = CAVV, but no VbV chargeback protection	7 <u>U.S. Note</u> : Because the CAVV was not valid for a U.S. Issuer, BASE II requires acquirer to submit an ECI 7 in BASE II	Not Applicable	RC 75/RC 83 Not Blocked	Research needed values, including ECI and CAVV; a PARes message Note: Some non- an Attempts PAR Server or ACS m which entitles the 6 with no CAVV in Request.	the Authenticat acquirer will nee from merchant. -U.S. issuers wi les = A. The Vis ay return a VEF merchant to su	ion Status, d a copy of ill not return a Directory Res = N ubmit an ECI
5. Attempted	Authenticatio	on by Merchant and	Card Is a Comm	ercial Card or	Anonymous Prepaid (Card		
6	Yes	B = Excluded Card Type (Commercial or anonymous Prepaid card)	7 See comments in PARes processing section to the right.	Not Applicable	RC 75/RC 83 Not Blocked	Research needed CAVV Results Co means that a Cor presented and At apply. BASE II re submit an ECI 7. to being charged Int'I Note: For a n changes the ECI even though an E	ode value. A val mmercial card v tempts process quires the acqu This transaction back. non-U.S. issuer to 7 for a Comr	lue of B vas ing does not irer to n is subject , BASE II nercial card,
to chargeback Authorization Results Code there was a C	s for Reason C Response, issu value returned AVV in the Aut	Code 75 or 83. If, how uers will be permitted in the VisaNet Author horization Request a	vever, there were to charge back o prization Respons nd it the same va	processing issu lisputed transac se. Acquirers ma lue was returne	herchant attempted to a les as indicated by the tions. Acquirers should ay need to request docu d in the PARes. If the n er can Represent along	CAVV Results Cod start dispute reseat mentation from the nerchant provides of	le value in the V arch by reviewin e merchant to d documentation	/isaNet g the CAVV etermine if
above were m	ARes with an Attempted Authentication <u>or</u> a VERes = N was received, the acquirer can Represent along with supporting documentation. If an acquirer receives a Pre-Compliance request to dispute an electronic commerce transaction and research determines all transaction requirements above were met, the acquirer may respond that VbV attempted authentication transactions are not eligible to be charged back. Documentation includes he PARes transaction with the Authentication Results Value or the VERes = N transaction.							

13 For Acquirers

13.1 Acquirer Role in Verified by Visa

To support acquirer and merchant participation in the Verified by Visa program, acquirers **must** perform specific functions and be prepared to assist their merchants in the following areas.

Step 1. Sign Up Merchants

Solicit and register merchants for participation in the Verified by Visa service. Provide guidance and support for their implementations.

Step 2. Ensure Operating Regulation Compliance

Ensure that participating merchants comply with all *Visa International Operating Regulations* pertaining to the Verified by Visa service, and that such requirements are included in their merchant agreements.

Step 3. Assist Merchants with MPI Plans

Assist merchants in evaluating various Merchant Server Plug-in (MPI) 'build or buy' and 'hosted' options for enabling their participation in the Verified by Visa program; ensure that the MPI implementation scenarios selected by merchants are consistent with acquirer processing requirements and policies. Refer to Chapter 9, *MPI Implementation Options*.

A list of vendors that have successfully completed required compliance testing with Visa of their MPI software can be downloaded at:

https://partnernetwork.visa.com/vpn/global/category.do?categoryId=85&documentId=117&userRe gion=1

Step 4. Support Product Integration Testing

Merchants, or their contracted payment service provider, are required to evidence the production readiness of their Merchant Server Plug-in prior to activation in Verified by Visa. Product Integration Testing (PIT) of the merchant's Merchant Server Plug-in by Visa has been designed to confirm this production readiness state.

A User Guide and a Policies and Procedures manual governing PIT usage is available to members and merchants. These publications describe steps to be taken by acquirers and merchants to conduct and validate the results of Product Integration Testing. Contact your Visa regional representative for additional information.

For additional information on both merchant testing and Verified by Visa testing services provided by Visa, see Chapter 10, *Implementation Considerations*.

Step 5. Submit Merchant Data for Visa Directory Server

U.S. acquirer BINs are set up automatically in the Visa Directory Server; therefore, an acquirer does not need to request to have their acquiring BINs set up in the Visa Directory Server. Because the U.S. Region uses client digital certificates for merchant authentication, there is no need for additional merchant data to be loaded in the Directory Server.

Refer to Chapter 8, *Digital Certificate Use*, for additional information about merchant authentication.

Step 6. Provide Merchants with Implementation Data

Provide each participating merchant with the following in preparation for their activation in the Verified by Visa service:

- The procedures for obtaining a Verified by Visa merchant digital certificate.
- The URL of the Visa Directory Server Provided to the acquirer by Visa and transmitted to the merchant over a secure channel as defined by Visa.
- Visa-Issued Certificate Used by the MPI to validate the issuer signature in the payment authentication response message from the Access Control Server (ACS). (Refer to Section 2.2, *Software Components*, for a description of the ACS and Section 3.2, *Online Purchases*, for a description of its role in 3-D Secure PARes processing.)
- Details on how to use and obtain the Verified by Visa marks Acquirers should provide merchants with details on how to obtain the Visa Product Brand Standards and Verified by Visa marks for use on their website. Acquirers may access Visa Online to get a copy of the Verified by Visa Merchant Toolkit with information about the Verified by Visa logo, the "Learn More" symbol, the "Activate Now" symbol, and usage guidelines.

Step 7. Provide Authorization Support

Provide traditional authorization and BASE II transaction processing.

Refer to Section 13.3, *Acquirer Processing Requirements*, in this chapter and Chapter 5, *Authorization Processing*.

Step 8. Support Dispute Resolution

Provide assistance to merchants in the resolution of disputes. Refer to Chapter 12, *Dispute Resolution*.

Step 9. Advise Visa Directory Server of Merchants to Remove

Immediately contact your Visa Representative to delete from the Visa Directory Server any terminated merchant, suspect merchant, or any merchant that fails to comply with the requirements of the merchant agreement governing merchant participation in the Verified by Visa program.

13.2 Visa Directory Server: Acquirer and Merchant Registration

Acquirer Set-Up

U.S. acquirer BINs are set up automatically in the Visa Directory Server; therefore, an acquirer does not need to request to have their acquiring BIN(s) set up in the Visa Directory Server. No additional set-up is required for acquirers.

Merchant Registration

The U.S. Region uses client digital certificates for merchant authentication. As a result, there is no need for additional merchant data to be loaded in the Directory Server.

Merchant Authentication and Certificates

Merchants are authenticated to the Visa Directory Server in 3-D Secure by using their client certificate. All Verified by Visa digital certificates are provided to merchants by their acquirer.

The acquirer also provides the Visa 3-D Secure Root Certificate and other Visa-issued certificates, obtained from the Visa to its merchants. The Visa 3-D Secure Root Certificate is used by the merchant for validating the issuer's digital signature in the PARes message.

13.3 Acquirer Processing Requirements

Acquirer Authorization Processing

The acquirer will receive the Electronic Commerce Indicator (ECI) value in the authorization message sent from the merchant and map it to the existing VisaNet authorization request message format: BASE I field 60.8 or SMS field 63.6. The ECI is not returned in a VisaNet Authorization Response.

Acquirer BASE II Processing

The acquirer will map the ECI value to Position 116 of the TCR1 sub-record in BASE II Draft Data.

Acquirers **must** also ensure that a new BIN-level flag, indicating Verified by Visa participation, is set to \mathbf{Y} (yes).

Transaction Identifier

The transaction identifier (XID) is a unique tracking number set by the merchant and sent to the ACS in the Payer Authentication Request (PAReq) message.

CAVV

The Cardholder Authentication Verification Value (CAVV) is a cryptographic value derived by the issuer during payment authentication that can provide evidence of the results of payment authentication during an online purchase. Issuers **must** include this value in each Payer Authentication Response (PARes) message sent to the MPI in which the Transaction Status value is either **"Y**" (Authentication Successful) or **"A**" (Attempts Processing Performed). The CAVV **must** be included in the VisaNet authorization message in order for the merchant to receive chargeback protection for U.S. and inter-regional transactions.

- Acquirers must:
 - Modify their systems, if necessary, to receive the required 3-D Secure fields.
 - In addition, acquirers **must** support and certify for the following V.I.P. fields:
- Field 126.9—TransStain (3-D Secure CAVV) that carries CAVV data. The use of Field 126.9 will be determined by the 3-D Secure issuer's access control server (ACS) protocol for authentication and attempts. Both the CAVV and Authentication Tracking Number (ATN) information are included in the same field.
- Field 44.13—CAVV Results Code that carries the results of validating the CAVV.
- Field 60.8—Additional POS Information, positions 9–10, that carries the MOTO/ECI for BASE I.
- Field 63.6— Chargeback Reduction/BASE II Flags, position 4, which carries the MOTO/ECI for SMS.
- **Field 126.8**—Electronic Commerce Transaction Identifier (XID). This field is recommended for support, but required when an ACS has returned a CAVV, Usage 2 of Field 126.9.

Refer to Chapter 5, *Authorization Processing*, for more information about CAVV, the PARes Fields for Authorization Requests, and CAVV processing.

3-D Secure Response Mapping Exhibit

Refer to Table 5-2, *3-D Secure Response Mapping Exhibit*, for a list of the ECI values related to 3-D Secure processing scenarios and their associated chargeback rights.

13.4 Sample Acquirer Project Plan

Table 13-1 lists the sample project plan used by acquirers for Verified by Visa Implementations.

Table 13-1. Sample Acquirer Froject Fran	Table 13–1:	Sample Acquirer Project Plan
------------------------------------------	-------------	------------------------------

ID	Task Name	Resource
	Acquirer Preparation: Verified by Visa Participation	
1	Identify business manager, project manager and multi-discipline team members.	Business Unit Owner
2	Scope high-level resource requirements for participation in Verified by Visa service.	Business and Project Managers
3	Evaluate feasibility of hosting MPI service for participating merchants.	IT Staff and Business/Project Managers
	Marketing and Promotion to Internet Merchant Base	
4	Develop and distribute Verified by Visa service highlights brochure to Internet merchants.	Marketing
5	Conduct Verified by Visa service promotion meetings for merchants.	Sales and Product Teams
6	Provide merchants with list of MPI vendor options.	Sales Team
7	Develop promotional Verified by Visa service Website; features, FAQs, and sign-up forms.	Product Manager
8	Propose Verified by Visa participation messages for merchant Websites.	Product Manager, Marketing
	MPI Technical Assessment	
9	Conduct cost/benefit and risk analysis of providing hosted MPI service.	Business Manager, Risk Management
10	Review compliant MPI vendor products; costs, features, and integration effort.	IT Staff
11	Assess offering and/or mandating acquirer hosted 3-D Secure Validation service.	Business Manager, Risk Management
12	Make 'Go'/'No Go' decision on hosted MPI and/or Validation service offering.	IT, Business and Project Managers
13	Notify merchants of acquirer decision not to host MPI or Validation service.	Business Manager

Table is continued on the next page.

Table 13–1:	Sample Acquirer Project Plan (Continued)
-------------	------------------------------------------

ID	Task Name	Resource
14	Develop, test and implement acquirer code to handle 3-D Secure transaction values.	IT Staff
	Acquirer and Merchant Registration Support in Verified by Visa	
15	Acquirer communication to Visa Representative of plans to implement Verified by Visa. Acquirer to confirm VisaNet readiness to process Visa authorization, settlement and clearing transactions that meet CPS e-Commerce requirements.	3-D Secure Operations
16	Amend merchant contracts to mandate compliance to 3-D Secure and Verified by Visa service requirements.	Legal and Sales
17	Register any Service Providers or High-Risk Merchants using the Member Management Application Service on Visa Online.	Implementation Manager
18	Solicit and register merchants in the Verified by Visa service.	Marketing and Operations
19	Track merchants' selection of MPI product/service solutions; ensure compliance	3-D Secure Operations
20	Promote Visa testing facility service; monitor testing and progress.	Visa System Test Facility and IT Staff
21	Validate final merchant readiness for Verified by Visa production via pre- activation test.	Implementation Manager
	Implementation and Production Support	
22	Provide merchant with merchant ID (new merchants) and client certificate.	Implementation Manager
23	Provide merchant with the URL of the production Visa Directory Server.	Implementation Manager
24	Provide merchant with Visa 3-D Secure Root and other Visa-issued certificates.	Implementation Manager
25	Activate merchant customer support; i.e., call center and problem escalation	Implementation Manager
26	Ensure correct VisaNet processing for Verified by Visa transactions.	Implementation Manager
27	Perform authorization and clearing processing using the required Verified by Visa fields.	Implementation Manager

Appendices Section

A. Planning and Implementation Example for Merchant Plug-In

This appendix provides an example of the planning and implementation steps for merchants that purchase a Merchant Server Plug-in to integrate with the web storefront software at their location. A more general discussion is provided in Chapter 10, *Implementation Considerations*.

The following topics are discussed:

- A.1 Assessment and Preparation
- A.2 Merchant MPI Software Selection
- A.3 MPI Technical Review
- A.4 Software Installation Planning
- A.5 Software Integration
- A.6 Testing
- A.7 Pre-Production and Production Launch

The appendix concludes with a checklist of the steps discussed.

A.1 Assessment and Preparation

Step 1. Decide Whether to Participate

In this phase, the merchant determines its interest in participating in the Verified by Visa program. This process begins with a joint review between the merchant and its acquirer or merchant processor of the features and benefits of Verified by Visa and the requirements for participation as defined in this guide.

Step 2. Review Activities

Following the merchant's decision to participate, the merchant conducts an initial review of the major activities to be performed and the necessary skills and disciplines required to plan and execute the implementation process.

Step 3. Establish Project Team

A project team is established that includes a business manager, a project manager, and representatives of various functional areas; including marketing, legal, operations, customer support, risk, and information technology.

Step 4. Develop Project Plan

A project plan is created that defines the major activities, tasks, dependencies, dates, and resources required to produce the deliverables to implement Verified by Visa processing within the merchant's environment. Some of the key activities and tasks that will require attention are:

- Development of the schedule for interim checkpoint reviews of the project plan
- Selection of an MPI software vendor
- Determination of MPI implementation location; that is, at merchant, payment service provider, or acquirer location
- Installation, integration, and testing of the MPI
- Development of dispute resolution procedures
- Obtaining merchant certificate, URL of the production Visa Directory Server, and Visa 3-D Secure Root Certificate from the acquirer
- Development of production rollout plans

A.2 Merchant MPI Software Selection

Step 1. Obtain Names of Software Solution Providers

A list of software solution providers is available at the link below. These vendors have developed 3-D Secure Merchant Server Plug-in (MPI) software and have successfully completed the required Visa compliance testing, as defined in the document *3-D Secure: Compliance Testing Facility – Policies and Procedures*.

https://partnernetwork.visa.com/vpn/global/category.do?categoryId=85&documentId=117&userRe gion=1

Step 2. Identify Technical Team

The merchant identifies the technical team responsible for the evaluation of the software of the 3-D Secure technology solution providers.

Step 3. Evaluate Solutions

The MPI software vendors present their respective solutions and associated merchant integration process documentation to the merchant for review and discussion. Joint review of the software options and the completed merchant environmental will help the merchant to select the software that best matches his business and technology needs.

A key aspect in the selection of the MPI will be an assessment of its compatibility, and integration requirements, with the merchant's existing software. Modifications to existing merchant software to implement Verified by Visa processing will vary based on a given merchant's commerce server installation and the Merchant Server Plug-in software solution chosen. At a minimum, the

merchant commerce server **must** be able to perform the following functions to enable it for Verified by Visa processing:

- Prepare all data relevant to the authentication and ensure the data is made available in the form where the final "Buy" page or "Check Out" button is present.
- Present authentication data to the Merchant Server Plug-in; the method for doing so being determined by the specific software functionality, attributes of a vendor MPI, and by the merchant's existing commerce server environment.
- Handle the return values presented by the Merchant Server Plug-in after the MPI receives the authentication response message.

See Table 10-1 for the Required Merchant Implementation Checklist.

Step 4. Select Solution

The merchant selects the software product that best enables the merchant's participation in the Verified by Visa program. After appropriate review, the merchant executes the vendor's software license agreement. This agreement should detail the vendor's commitment to provide support, either under the license agreement or separate professional services agreement, for software installation and future software upgrades as required by the merchant.

A.3 MPI Technical Review

Step 1. Provide Questions to Vendor

In preparation for a joint review with the MPI software vendor, any outstanding questions regarding the Merchant Server Plug-in software and a schematic of the merchant's existing merchant commerce platform should be forwarded to the vendor. This will allow for an assessment, from the vendor's perspective, of the probable steps required to achieve merchant Verified by Visa participation at the lowest cost to the merchant, and an estimate of the timeframe to complete installation and integration of the software solution at the merchant site. It will also serve to ensure that any technical barriers to merchant participation are identified and remedial measures developed.

Step 2. Conduct Technical Review

A technical review meeting is scheduled between the merchant's technical team and the vendor. The purpose of this meeting is to conduct an in-depth review of the vendor Merchant Server Plugin solution and the context of the existing merchant commerce server installation, and identify each of the steps required for implementing the vendor's MPI Verified by Visa software solution at the merchant location. At the conclusion of this meeting, the merchant should understand the technical requirements for integrating the Merchant Server Plug-in. Conversely, the vendor should have a complete understanding of the merchant environment.

A.4 Software Installation Planning

Step 1. Decide Who Will Install

Based on the outcome of technical reviews with the vendor and internal assessment of options, the merchant will decide who will install the MPI software. In most instances, the options for installation are the merchant's internal engineering resources, contracted resources, or execution of a professional services agreement with the software vendor. Once this decision is made, the process of installing the Verified by Visa software can begin.

Step 2. Define Resources

If the merchant elects to implement the software with internal resources, the merchant needs to ensure agreement with the technology provider as to the level of support that the vendor will make available. Conversely, if the merchant decides to have contracted resources or the vendor install the software, the merchant should identify a technically proficient staff resource to liaise with the contracted resources or the vendor regarding questions specific to the merchant environment and to monitor the progress of software installation.

A.5 Software Integration

Step 1. Develop Integration Plan

A detailed MPI software integration plan is created, listing the detailed implementation tasks to be completed, estimated start and completion dates, and the resource responsible for completion of each activity.

Step 2. Install Software

The responsible parties perform the defined tasks necessary to install the software in the merchant's development environment. After installation, testing will be conducted to ensure the quality of the integration of the vendor software before moving it into production.

Step 3. Implement Required Interface Changes

The merchant will need to identify, plan, schedule, and execute all required changes to server configurations, DNS, routing tables, firewalls, procedures, and other operational matters.

A.6 Testing

Step 1. Perform Unit Testing

The merchant performs unit testing to ensure that the software was successfully installed. During unit testing, the merchant software communicates with test servers to test Verified by Visa transaction processing.

Step 2. Perform Other Internal Testing

After unit testing has been successfully completed, the merchant performs additional testing according to internal requirements and testing procedures, including regression, stress, and QA testing.

Step 3. Conduct Product Integration Testing

Merchants operating MPIs, and third parties operating MPIs on behalf of merchants, are required to evidence proof of the production readiness of their MPI implementation prior to entering live production in the Verified by Visa program.

Visa provides the "Product Integration Testing" facility, also known as PIT Testing, to test the production readiness of MPI implementations prior to entry into production Verified by Visa. Refer to Section 10.4, *Requirements for Pre-Production Readiness via Production Integration Testing (PIT)*.

A.7 **Pre-Production and Production Launch**

Completion of successful testing will ensure merchant confidence that the Verified by Visa software functionality and its integration into the merchant commerce server are yielding the expected results, and that the merchant's processing environment is stable.

The merchant is now ready to proceed with the final pre-production steps described below.

Step 1 Determine Production Date

Determine a production date and request that the acquirer have necessary merchant data populated in the Visa Directory Server by that date.

Step 2. Obtain Data From Acquirer

Request and receive from the merchant's Visa acquirer:

- The URL of the production Visa Directory Server
- The Visa 3-D Secure Root Certificate and other Visa-issued certificates
- The procedures for obtaining a merchant digital certificate

• The Verified by Visa Mark, and information on graphic standards and guidelines for displaying the mark

Step 3. Install Visa 3-D Secure Root Certificate

Install the Visa 3-D Secure Root Certificate in the MPI.

Step 4. Obtain the Verified by Visa Merchant Digital Certificate

Obtain the Verified by Visa merchant client digital certificate and load it into the MPI. Acquirers will find the forms to request merchant certificates via Visa Online. Click on the *Products and Services* tab, then, click on the "Verified by Visa" link. On the left side, click "For Acquirers;" the certificate request form is in the list of "Useful Acquirer and Merchant Tools."

Step 5. Point MPI to Production Visa Directory Server

Make necessary code changes to enable the MPI software to point to the production Visa Directory Server.

Step 6. Go Live

Commence processing in the production Verified by Visa program.

A.8 Checklist

ID	Task Name	Resource
	Assessment and Preparation	
1	Decide whether to participate	Merchant, acquirer
2	Review activities	Merchant
3	Establish project team	Merchant
4	Develop Project Plan	Project team
	MPI Software Selection	
1	Obtain names of software solution providers	Project team
2	Identify technical team	Project team

Table A–1: Example Planning and Implementation Checklist

Table is continued on the next page.

	Task Name	Resource
3	Evaluate solutions	Technical team
4	Select solution	Project and Technical teams
	MPI Technical Review	
1	Provide questions to vendor	Technical team
2	Conduct technical review	Technical team, technology provider
	Software Installation Planning	
1	Decide who will install	Project team
2	Define resources	Project team, technology provider
	Software Integration	
1	Develop integration plan	Project team with technical team and/or technology provider
2	Install software	Technical team and/or technology provider
3	Implement required interface changes	Project team with technical team
	Testing	
1	Perform unit testing	Technical team
2	Perform other internal testing	Technical team
3	Conduct Product Integration Testing	Technical team
	Pre-Production and Production launch	
1	Determine production date	Project team, acquirer
2	Obtain data from acquirer (Visa 3-D Secure Root Certificate, merchant's digital certificate, etc.)	Technical team, acquirer
3	Install Visa 3-D Secure Root Certificate	Technical team
4	Install merchant digital certificate	Technical team
5	Point MPI to production Visa Directory Server	Technical team
6	Go live	Technical team

Table A–1:	Example Planning and Implementation Checklist (Continued)
------------	-----------------------------------------------------------

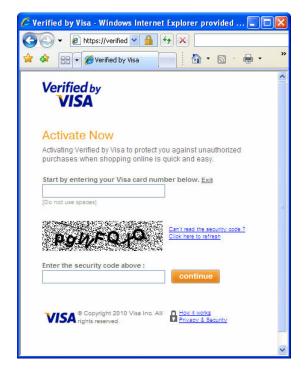
B. Verified by Visa Activation Anytime

Activation Anytime is a capability designed to enable issuers to activate cardholders at various Internet sites, including participating merchants. It is easy for participating merchants to implement support for Activation Anytime. The only requirement is the placement of Verified by Visa banners or buttons for Activation Anytime. When the cardholder clicks on the banner or button, the Verified by Visa Landing Page appears. The transaction flow is described below.

Step 1: Click to Activate

When cardholders click on a Verified by Visa banner or button for Activation Anytime, the Activation Anytime Landing Page appears. This page provides a brief description of Verified by Visa and benefits for activating their Visa card as shown in Figure B-1.

Figure B-1: Activation Anytime Landing Page



Cardholders are given the opportunity to enter their Visa card numbers to activate immediately. When the card number is entered, the cardholder is presented with one of several pages: an issuer activation page or an issuer enrollment page. If the issuer is not participating in Verified by Visa, a "Service Not Available" page is presented. These pages are illustrated in the following sections.

Step 2: Verify Identity and Activate

When customers enter their card numbers, the Activation Anytime server performs a validity check that it is a valid Visa card number. The customer is then presented with the issuer's activation page. The issuer may request identity information, as shown in Figure B-2, to authenticate the cardholder.

Figure B-2: Sample Issuer Activation Page

6			
File Edit View Favorite	es Tools Help		
Adidness 🙋 http://onlinestore.	com 🔹 🔗 Go 🛛 Links 🛎 Customize Links 🔹 Free Hob	mail 🛛 Windows Media 🤞	
\$= Back • ⇒ • ③ ③	🕼 Q Search 🗟 Favorites 🔇 History 🔄 - 🎒 🕅 - 📄		
OnlineStore	Your Account W Cart & Checkout Help		
	🚰 Activation Anytime - pan entry - Microsoft Internet Explore 🔳 🗐 🗙	1	
Photo	Fle Edit Vew Favortes Tools Hel:		
Electronics Phone Center	Address 🛃 https://verified.visa.com/aam/data/1/anding.adtivs 💌 🔗 Sc 🛛 Links 🚿		
Search	📙 🕂 Rack – 🔿 – 🥥 🚮 🖓 Searn 🔛 Favorites 🏈 History 🎽		
	Verified by		
Welcome	VISA Member Name	Verified by	
Books	VIDA	VISA	
		Activate now	
• Swing Siets	Please Verify Your Identity	ore Products at	
Outdoor Play	Complete this form and then click continue.	ing Prices	
Photo Center		opping	
Digital Cameras Camcorders	Last d daile at COM, your your	arm more.	
My Photos	Last 4 digits of SSN: XXX-XX-	L ess	
Video Games	Signature panel code: The last3 digits on		
Music	Visa card expiration date: / [MM/YY]		
Movies	Email address:		
• <u>DVD</u> • <u>VHS</u>			
Home	Continue Cancel	1 2	
 Furniture & Decor Appliances 		ран (так) (
	By clicking Continue, you agree to these Terms & Conditions		
<u>Electronics</u> <u>Computers</u>		ertainment.	
 TV, Audio & Video DVD Pla vers 	🖹 🕒 🙆 🙆 Internet	J	
Cift Bogicta		NE ORNERAL	
2] Contraction (Contraction of Contraction of Contr			

Step 3: Create Password

To complete the activation, the cardholder is requested to create a password for use at participating online merchants as shown below in Figure B-3.

Figure B-3: Sample Password Creation Page

ididress 🐖 http://onlinestore.c	om 🔻 🖉 Go 🛛 Links 🚑 Customize Links 🖉 Free Hotmail 🖉 Window	is Medi
	쇼 @_Search @Favorites @History 원 · 글 ඕ · 글	
OnlineStore	Your Account @ Card & Checkout Stele	
Electronics Photo Center Stearch	Address (E) lithes //verified vites com/samidital filancina software (Passe Lunis *) Periodi	
Welcome Books	Verified by VISA Member Name Verified VISA	A ´
Toys • Swing Sets • Outdoor Play Photo Center	Create Your Password You'll use your password to make purchases at participating online stores.	
Digital Cameras <u>Camcorders</u> <u>My Photos</u>	Your password can be (c) to (cc) characters. Use any combination of letters, number or symbols, Do not us space. Be sure to keep your nasword in a safe to lace.	
<u>Viideo Games</u> Music	Create password:	
Movies DVD VHS		
Furniture & Decor Appliances	Continue 🔽 Hele. Ext.	
<u>Computers</u> <u>TV, Audio & Video</u> DVD Pla vers	artainment.	

Step 4: Confirm Activation Successful

After the activation is completed, the cardholder is presented with a confirmation page that the activation was successful.

Figure B-4: Sample Activation Successful Page



Upon clicking the Close button, the cardholder is returned to the merchant site.

Note:

Non-Participating Issuer. If the issuer does not participate in Verified by Visa, the customer is presented with a "Verified by Visa Not Available for This Card" page and returned to the merchant site.

What's Required for Merchants to Support Activation Anytime

Participating merchants may support Activation Anytime by displaying Visa-provided signage for Activation Anytime. When the cardholder clicks on the signage, a secure Activation Anytime browser window will be opened with the Visa URL visible and SSL lock displayed with the corresponding Visa digital certificate information. These security cues are important for customers to be able to ensure that they are connecting to the authentic <u>www.verified.visa.com</u> server – helping to reassure customers of the confidentiality of their information.

As shown in Figure B-1, the browser window is smaller than a full browser window, so the customer maintains visibility of the merchant site. When the browser window is closed, the customer automatically returns to the merchant site.

The Verified by Visa signage for Activation Anytime will be available for merchant implementation. Acquirers and merchants will find guidelines and logos in the *Verified by Visa Merchant Toolkit*, available at Visa.com.

C. Best Practices: Fraud Screening

There are a wide variety of fraud screening services and practices available that will help merchants assess the risk of a transaction and increase the likelihood that the person making the transaction is the legitimate cardholder with a valid card. In addition to Verified by Visa, fraud screening tools may be developed internally by merchants or their acquirer, or may be purchased from a third party.

C.1 Reducing Risk

The following best practices will help merchants reduce the risk of fraud:

- In addition to Verified by Visa, layer fraud screening tools to identify high-risk transactions or patterns of transactions.
- Do not process transactions with high-risk characteristics, such as:
 - Transactions with data that matches those stored on gray lists.
 - Transactions that exceed velocity limits and controls.
 - Transactions that generate either an Address Verification Service (AVS) or Card Verification Value 2 (CVV2) mismatch.
 - Transactions that fit high-risk profiles.
- Verify the cardholder's address when a transaction generates an AVS mismatch by reference to voters' roll information, local directories, or directly with the cardholder.
- Screen for high-risk shipping addresses, such as mail drops, post office boxes, prisons, hospitals, and so forth.
- Monitor for orders placed with multiple and specifically sequential card numbers or a disproportionate number of orders from one issuer.

C.2 Identifying Fraudulent Behavior

The following characteristics could indicate fraudulent behavior.

- For international transactions, assess risk based on:
 - Type of goods purchased
 - Transaction amount
 - Country where the card was issued
 - Country where the merchandise is to be shipped.

A merchant's acquirer should be able to offer help with this.

C.3 Possible Risk Indicators

Visa recommends merchants put into place in-house policies and procedures for handling irregular or suspicious transactions (for example, unusually large orders).

Sales staff should be trained to recognize suspicious orders and given clear instructions on the steps they should take to verify these transactions. Experience suggests that there are certain characteristics that can be tip-offs to possible fraud. One of these characteristics is rarely an indication of fraud. However, when several are present in the same purchase, it is much more likely to be a fraudulent transaction.

The possible risk indicators include:

- First time customer
- High value orders or orders that are larger than normal
- Customer requests urgent delivery
- Ordering randomly or in multiples
- Providing different ship-to and billing addresses
- Paying with multiple cards

If one or more of the following indicators is present in the transaction, it may indicate *increased* risk:

- First time customers—The risk of fraud is less when dealing with repeat customers.
- Large orders—Orders that are larger than normal may indicate fraud. Also, high value purchases for items such as jewelry or electrical goods are often the target for fraud as they can easily be resold. Greater vigilance is required for these types of transactions.
- Multiple orders—Orders consisting of several purchases of the same item may arouse suspicion.

- Suspicious card combinations—A variety of payment card combinations might give rise for concern and further investigation, for example:
 - a. Transactions made with cards that have similar account numbers.
 - b. Orders shipped to a single address, but purchased with various cards.
 - c. Multiple transactions on a single card over a very short period of time.
 - d. Multiple transactions made with several cards with a single billing address, but multiple shipping addresses.
 - e. A single transaction in which the customer wants to pay with multiple cards. More than one or two cards may well indicate a fraudulent transaction.
- Rush orders—Urgent requests for quick or overnight delivery. The customer who 'needs it yesterday' – are another sign of possible fraud. While often perfectly valid, rush orders are one of the common characteristics of 'hit and run' fraud schemes aimed at obtaining merchandise for quick resale.
- Suspicious shipping address—Scrutinize and flag any order with a ship-to address that is different from the billing address on the cardholder's account. Requests to ship merchandise to post office boxes or an office address are often associated with fraud. In addition, merchants should keep lists of postcodes where high fraud rates are common and verify any order that has a ship-to address in these areas.

C.4 When Fraud is Suspected

If fraud is suspected, merchants should contact the customer and ask for additional information to verify the order. Validate telephone numbers with addresses and check lists related to previous chargeback problems, and so forth.

The following steps may help to verify suspect transactions:

- Check the customer's personal information.
 - Request day and evening telephone numbers and verify them through directory assistance or by calling the customer directly.
 - If possible, merchants should also compare the billing and ship-to address on the order with the address used for mailing the customer any catalogues or other marketing materials.
- Separately confirm the order with the customer. Send a note to the customer via his/her billing address, rather than the 'ship to' address.

D. Verified by Visa Global Performance Enhancement Program

D.1 In Brief

In order to ensure the highest level of performance for the Verified by Visa program in the marketplace, Visa implemented the Verified by Visa Global Performance Enhancement Program. This program consists of standards that strengthen the performance of participating Verified by Visa issuers, acquirers, and merchants and it provides a framework to ensure standards and requirements are met by all participants. The Verified by Visa global performance standards consist of:

- Issuer Authentication Standards
- Issuer Activation Requirements
- Acquirer and Merchant Transaction Quality

This appendix provides information about Acquirer and Merchant Transaction Quality.

D.2 Verified by Visa Global Performance Standards

Merchant/Acquirer Transaction Quality

Verified by Visa was designed to act in conjunction with other fraud mitigation tools. Merchants/acquirers are not allowed to rely exclusively on Verified by Visa for fraud and risk mitigation. Instead merchants/acquirers **must** use an adequate combination of fraud screening and risk mitigation tools available to ensure fraud is managed to the lowest possible level.

Introduction

Participation in the Verified by Visa program requires merchants/acquirers to manage their related processes effectively and efficiently. This required management applies not only to the authentication of individual transactions; it also applies to how the merchant/acquirer uses decisioning logic relative to transactions eligible for the benefits provided by Verified by Visa.

Verified by Visa is designed to be an additional layer of security layer for issuers and merchants/acquirers to use in online purchase transactions. Just as issuers are expected to use all the tools they have at their disposal in the authentication and authorization processes, merchants/acquires are also required to apply appropriate risk mitigation necessary to protect their interests and the interests of the program. Merchants/acquirers are required to apply the same rigors as they would for any other non-Verified by Visa transaction.

Merchants/acquirers are expected to use an adequate combination of tools available, based on a merchant's business, to ensure fraud is managed to the lowest level possible. Visa provides merchants/acquirers with several tools to help manage fraud. AVS (Address Verification Service), CVV2 (Card Verification Value 2), and Verified by Visa are three examples. In addition,

acquirer/merchants are encouraged to conduct velocity checks, perform IP checking and use the variety of tools in the marketplace to assist in fraud mitigation.

Policy Definition

The goal of this policy is to act as an early warning system, and Visa will work closely with underperforming merchants/acquirers to manage their Verified by Visa program effectively. Through defined severity levels the program enables early detection of merchants experiencing potential Verified by Visa performance issues prior to a formal identification in any of the existing Visa merchant compliance programs (e.g., GMCMP, MFP). The early warning enables the capability to contain fraud before it reaches excessive levels.

Merchant identification will be based on a calculation consisting of confirmed fraud and chargebacks.

The merchant threshold calculation is indicated below. There will be separate calculations for ECI **5** and ECI **6** transactions, each relative to the sales volume for the particular ECI. All identifications will be based on reported date, not purchase date, and will be cross-border activity only.

((TC40) – (Chargeback RC 83)) + (Chargeback RC 30, 77, 75, 85)¹

Sales Volume

Any merchant that meets the following criteria will be subject to conditions specified by the corresponding severity level indicated below:

- Exceeds 25 exception transactions for the reported month, AND
 - Exceeds merchant calculation to sales rate of 1% (based on count), OR
 - Exceeds an overall merchant calculation amount of \$200,000

Table D-1. VbV Global Performance Program Standards

Actual Rate	Severity Level
1.0 to 2.24%	Alert / Warning
2.25% and Above	Extreme Warning
Above \$200,000	Alert / Warning
Above \$300,000	Extreme Warning

¹ Names for the reason codes are as follows: RC 83 – Fraud Card-Absent Environment; RC 30 – Services Not Provided or Merchandise Not Received; RC 77 – Non-Matching Account Number; RC 75 – Transaction Not Recognized; RC 85 – Credit Not Processed.

Escalation Process

Alert / Warning

An "Alert / Warning" highlights that the acquirer/merchant is approaching an Extreme Warning level threshold. Any additional actions regarding this notification are at the sole discretion of Visa.

Extreme Warning

Once a merchant has been highlighted in the "Extreme Warning" threshold the following steps occur:

- 1. Visa will determine if the acquirer/merchant is in compliance with all the *Visa International Operating Regulations* governing Verified by Visa transactions. Visa will have 7 business days from original notification for this determination.
- 2. Visa will instruct the acquirer/merchant to implement necessary tools.
- 3. Visa also has the option of requiring the merchant to implement the appropriate Merchant Best Practices defined by Visa.
- 4. Merchants will be warned that if corrective actions are not taken, they may be subject to identification in any the Visa Compliance Programs (e.g., GMCMP, MFP, etc.) and whatever fines and penalties are associated with those compliance programs.
- 5. If the merchant complies with all requirements from Visa but the merchant is still subsequently identified by a Visa Compliance Program (i.e., GMCMP), the Visa Representative has the option to appeal any fines and/or penalties that may be levied against the merchant resulting from that identification (i.e. fines for GMCMP) on behalf of the merchant.
- If merchant does not comply with requirements from Visa and is identified in any Visa Compliance Program multiple times², Visa has the option of permanently removing the merchant from the Verified by Visa Program.

Additional Information

For more information, please refer to the Visa Business Review article, "Visa Approves International Operating Regulation Revisions, Verified by Visa Global Performance Enhancement Program" published in November 2007, or contact your Visa Representative.

² If a Merchant is identified in Merchant Fraud Performance, is re-activated, and then is re-identified; Visa has the right to remove the Merchant from the service with no possibility of re-instatement.

Glossary

This section defines selected terms related to the Verified by Visa (VbV) program.

3-D Secure

A specification developed by Visa to improve transaction performance online and to accelerate the growth of electronic commerce by enabling issuers to verify a cardholder's account ownership during an online purchase.

AACS

See Attempts Access Control Server.

Access Control Server

A server hardware/software entity that includes a database of account and password information for cardholders registered for the Verified by Visa program. The ACS is operated by the issuer or the issuer's processor. In response to Visa Directory Server inquiries, the ACS verifies cardholder participation in the issuer's Verified by Visa program, receives authentication requests from merchants, authenticates the cardholder during online purchases, and provides digitally-signed authentication response messages (containing the authentication results and other Verified by Visa data) to the merchant and to the Authentication History Server.

Account Holder File

A master account database for registered users that contains all information required for authenticating cardholders during an online purchase. This database is stored in the ACS.

Acquirer

A Visa member financial institution that enters into a contractual relationship with a merchant for the purpose of accepting Visa cards. The acquirer determines the merchant's eligibility to participate in Verified by Visa.

Acquirer Domain

The systems and functions of acquirers and merchants in 3-D Secure. See also Issuer Domain and Interoperability Domain.

ACS

See Access Control Server.

AHS

See Authentication History Server.

Attempts Access Control Server (AACS)

A server hardware/software entity that provides an attempted authentication response for cardholders not registered for the Verified by Visa program. Like an ACS, an AACS can be operated by the issuer, the issuer's processor, or Visa on behalf of the issuer. The AACS does not provide cardholder authentication but generates an attempted authentication response and a CAVV that is sent to the merchant for inclusion in the authorization message, as proof that authentication was attempted.

Attempts Functionality

The process by which the proof of an authentication attempt is generated, when payment authentication is not available.

Authentication

The process by which cardholder ownership of the payment card account is validated by the card issuer in accordance with the Verified by Visa program rules and processes.

Authentication History Server

A 3-D Secure system component responsible for receiving, storing, and reporting on copies of all Payer Authentication Response messages. The Authentication History Server is operated by Visa.

Authentication Request

See Payer Authentication Request.

Authentication Response

See Payer Authentication Response.

Authorization

The process in which the issuer, or a processor on the issuer's behalf, approves or denies a Visa card transaction.

Bank Identification Number

A six-digit number assigned by Visa and used to identify a Visa member or processor for authorization, clearing, and settlement.

BIN

See Bank Identification Number.

BID

See Business I.D.

Browser

A client program that allows users to read hypertext documents on the World Wide Web and navigate between them. Examples are Microsoft Internet Explorer, FireFox, and Safari.

Business I.D

A unique identification number assigned by Visa U.S.A to members and registered third-party service providers.

Cardholder

An individual to whom a Visa payment card is issued by a Visa card issuer, or who is authorized to use this Visa card.

Cardholder Authentication Verification Value

Cardholder Authentication Verification Value (CAVV) is a value generated by the ACS using the same algorithm as CVV. CAVV is created using different data elements, then signed by the issuer and sent to the merchant in the Payer Authentication Response (PARes) message.

CAVV

See Cardholder Authentication Verification Value.

Certificate

An electronic document that contains the public key of the certificate holder and which is attested to by a Certificate Authority and rendered unforgeable by cryptographic technology (signing with the private key of the Certificate Authority).

Certificate Authority

A trusted party that issues and revokes certificates.

Chip Card

A payment card with a built-in microprocessor and memory used for identification and financial transactions. When inserted into a reader, it can exchange data with an issuer ACS.

Cryptography

The process of protecting information by transforming it into an unreadable format. The information is encrypted using a key that makes the data unreadable, and then decrypted later when the information must be used again.

Customer Service Representative

Employees or agents who are responsible for primary customer support; can be employees of an issuer, acquirer or merchant.

Digital Signature

A set of electronic data used to authenticate parties to a transaction.

Directory Server

See Visa Directory Server.

Interoperability Domain

The Visa operated systems that connect the issuer and acquirer domains. See also Acquirer Domain and Issuer Domain.

lssuer

A Visa member financial institution that enters into a contractual relationship with the cardholder for issuance of one or more Visa cards. The issuer determines whether the cardholder is eligible to participate in Verified by Visa.

Issuer Domain

The systems and functions of issuers and cardholders in 3-D Secure. See also Acquirer Domain and Interoperability Domain.

Merchant

An entity that contracts with a Visa acquirer to originate transactions and that accepts payment cards. Each Visa merchant must have a Merchant Agreement with a Visa acquirer.

Merchant Commerce Server

A server hardware/software entity that handles all online transactions and facilitates communication between the merchant application and the Visa gateway.

Merchant Server Plug-in

A module integrated into merchant store-front applications used to process Verified by Visa authentication transactions. It provides an interface with the merchant commerce server.

Merchant Server Software

See Merchant Server Plug-in.

MPI

See Merchant Server Plug-in.

PAReq

See Payer Authentication Request.

PARes

See Payer Authentication Response.

Password Hint

When selecting the Verified by Visa password, the cardholder may also select a password hint. The cardholder may use the hint to help remember his/her password during an Internet transaction. The hint must not contain text that is included in the password.

Payer Authentication Request

A message sent from the merchant server software to the issuer ACS via the cardholder browser. The message requests the issuer to authenticate its cardholder and contains cardholder, merchant, and transaction-specific information.

Payer Authentication Response

A message formatted, digitally signed, and sent from the issuer ACS to the merchant server software via the cardholder browser, providing results of the issuer's Verified by Visa cardholder authentication.

Payment Gateway

A third party that provides an interface between the merchant/acquirer's payment system and VisaNet.

Personal Assurance Message

A message selected by the cardholder during the registration process that is displayed during the authentication process to indicate that the password request is from a valid source. The personal message is between 1 and 30 characters and must not contain text that is included in the password.

Proof of Attempted Authentication

See Attempts Functionality.

Registration Server

A server that manages cardholder registration in the Verified by Visa program. The registration server presents a series of questions via a Web interface to be answered by the cardholder and verified by the issuer or issuer designate. The registration server is operated by or on behalf of the issuer.

Secure Sockets Layer or SSL

A cryptographic protocol developed to confidentially transmit information over open networks such as the Internet.

Technology Provider

An entity that provides technical services in support of the Verified by Visa program.

Three-Domain Secure

See 3-D Secure.

Uniform Resource Locator or URL

Global address used for locating resources on the Internet.

VbV

See Verified by Visa.

VEReq

See Verify Enrollment Request.

VERes

See Verify Enrollment Response.

Verified by Visa

A program designed to improve the security of purchases made via the Internet, enabling issuers to verify cardholder account ownership during the online purchase. Verified by Visa is based upon the 3-D Secure technical specifications. Verified by Visa supports magnetic stripe Visa cards and Visa chip cards.

Verified by Visa Mark

The consumer mark developed specifically to signify merchant participation in the Verified by Visa program. To use the mark, merchants are required to follow guidelines (available from a merchant's Visa acquirer or merchant processor).

Verified by Visa Password

Selected by the cardholder during the registration process, the Verified by Visa password is used by the issuer to authenticate the cardholder during Internet purchases. The password must be between 4 and 12 characters long and may include numbers, letters, and/or printable characters but not spaces.

Verified by Visa Signing Certificate

The certificate used to digitally sign authentication responses sent from the ACS to a Verified by Visa merchant. Upon receipt, the merchant verifies the digital signature to ensure that the response was sent from an authorized ACS.

Verify Enrollment Request

A message sent from the merchant server software to the issuer ACS via the Visa Directory Server to verify whether the cardholder participates in the authentication program.

Verify Enrollment Response

A message sent from the issuer ACS (or the Visa Directory Server on its behalf) in response to a Verify Enrollment Request.

Visa Directory Server

A server hardware/software entity that is operated by Visa, whose primary function is to route authentication requests from merchants to specific Access Control Servers and to return the results of authentication.

VisaNet

Systems and services through which Visa delivers financial processing, authorization, clearing, and settlement services to members.

14 Index

3-D Secure Compliance and Testing, 6 3-D Secure Messages, 23-28, 40 3-D Secure Specification, 6, 13, 15, 59-60 3-D Secure Technology Providers, 5 Access Control Server, 16, 19-20, 64, 99 Acquirer Domain, 15-16, 99 Acquirer Materials, 5 Acquirer Project Plan, 80 Acquirers, 14, 44, 54-55, 59, 69, 76-79, 96, 99 ACS. See Access Control Server Activation Anytime, 50, 90 Activation During Shopping, 17 attempted authentications, 10, 16, 26-28, 72-73 Attempts Access Control Server (AACS), 100 Authentication, 8, 17, 32, 37, 72, 100 Authentication Data Limits, 39 Authentication Failed, 29, 50 Authentication History Server, 16, 21, 100 Authentication Identifier, 31 Authentication Results, 26 Authorization Characteristic Indicator, 37 Authorization Processing, 8, 22, 27, 29-39, 67, 100 Cache Messages, 28, 41 Cardholder, 14, 101 Cardholder Authentication Verification Value, 21-22, 29, 31, 33, 35, 79, 101 Cardholder enrollment, 17 Cardholder Information Security Program, 5, 43-44, 66,70 Cardholder Password, 104 CAVV. See Cardholder Authentication Verification Value CAVV Results Code, 79 Chargeback Protection, 10-11, 72

CISP. See Cardholder Information Security Program Commercial cards, 19, 27, 72 CPS/Electronic Commerce Preferred, 11, 36 Custom Payment Service, 11, 36 Custom Software Development, 60 delayed delivery, 37 Digital Certificates, 54-56 **Dispute Resolution**, 72-75 ECI. See Electronic Commerce Indicator Electronic Commerce Indicator, 21-22, 30, 33, 37, 78,97 Fraud Screening, 68, 93-95 Global Merchant Chargeback Monitoring Program, 69-70 Global Merchant Fraud Performance, 69-70 Hosted MPI Options, 59 Implementation Checklist, 66 Implementation Considerations, 57, 61-67 Inline Page, 46-48, 66 Installment Transactions, 39 International Transactions, 24 Interoperability Domain, 15, 16, 102 Issuer, 14, 102 Issuer Domain, 15, 102 Merchant Authentication, 19, 44-45, 55, 77 Merchant Benefits, 10 Merchant Category Codes, 28, 72 Merchant Certificate, 41, 54-55, 77, 84, 88 Merchant Chargeback Monitoring Program, 69-70 Merchant Materials, 5 Merchant Password, 27 Merchant Performance Standards, 51 Merchant Server Plug-In, 16, 18, 22, 29, 40-41, 53-54, 57-58, 61, 64, 82, 102

Merchants, 14, 44, 55, 57, 61, 68, 78, 96, 102	split shipment, 37	
Merchants Agreements, 44	SSL. See Secure Socket Layer	
MPI. See Merchant Server Plug-In	System Resiliency, 68	
Online Auctions, 39	Timeout Sequencing, 43	
PARes. See Payer Authentication	Trademarks, 1	
Payer Authentication, 20-21, 25-26, 29, 33, 35, 40,	Transaction Flow, 18-19	
50-52, 73, 79, 103	Transaction Status Values, 29	
Payment Card Industry (PCI) Standard, 5, 70	Transport Security, 56	
Performance Standards, 96	Verified by Visa Global Performance Standards, 70,	
Personal Assurance Message, 17, 103	96–98	
PIT Testing, 6, 63-64, 66-67, 87	Verified by Visa Mark, 4, 12, 49, 88, 104	
Pre-Authentication Messaging, 45, 66	Verified by Visa Merchant Toolkit, 5, 12, 50, 92	
Prepaid cards, 27, 72	Verified by Visa Overview, 7	
Reason Code 75/83, 10, 28, 72-73	Verified by Visa Publications, 4	
Record Keeping, 41	Verify Enrollment, 23-25, 27, 33, 40, 51, 53, 55, 104	
Recurring Transactions, 38	Visa Attempts Service, 16, 20, 24, 26	
Registration Server, 15, 103	Visa Certificate Authority, 54-55	
RIS Online, 69	Visa Directory Server, 16, 19, 20, 23, 27, 44-45, 54- 56, 78, 87, 104	
Risk Management, 5, 68, 93		
Secure Sockets Layer, 13, 56, 103	Visa Root Certificate, 29, 41, 54, 78, 84, 87	
Software Development Kit, 58	Visa Transaction Routing Service, 16, 20-21, 25	
Software Solution Providers, 84	VisaNet, 14, 104	