Verified by Visa Service Description

U.S. Region

October 2010

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. THE ISSUER, ACQUIRER, MERCHANT, OR PROCESSOR IS SOLELY RESPONSIBLE FOR ITS USE OF THE INFORMATION CONTAINED HEREIN.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROPRIETARY AND CONFIDENTIAL AND MUST BE MAINTAINED IN CONFIDENCE IN ACCORDANCE WITH THE VISA OPERATING REGULATIONS AND BY-LAWS.

Contents

About This Guide

This publication provides an overview of the Verified by Visa program, including a description of the business objectives, how Verified by Visa transactions work, and the key participants and their roles and responsibilities in Verified by Visa transactions.

Verified by Visa is a service designed to improve the security of purchases made via the Internet, enabling Issuers to verify a cardholder's account ownership during an online purchase. The technology platform for Verified by Visa is called the Three-Domain (3-D) Secure Protocol.

Trademarks

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

Audience

This guide is intended for U.S. participants, including

- Issuers and issuer processors
- Acquirers and acquirer processors
- Merchants

Document Organization

Chapter 1, Introduction—This chapter provides a brief overview of the Verified by Visa program, the 3-D Secure technology platform and key program components.

Chapter 2, Transaction Flow—This chapter describes the steps in a Verified by Visa authentication transaction.

Chapter 3, Linking Authentication and Payment—This chapter highlights the links between Verified by Visa authentication and Visa authorization and settlement transactions.

Chapter 4, Implementation Considerations—This chapter reviews some of the key considerations for issuers and acquirers as they implement Verified by Visa.

Resources and Tools

Documentation has been developed for issuers, acquirers and merchants to assist in understanding the 3-D Secure technology platform as well as Verified by Visa program requirements. The support materials are described below.

Verified by Visa Publications and Materials

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

- Verified by Visa Service Description
- Verified by Visa Issuer Implementation Guide
- Verified by Visa Acquirer and Merchant Implementation Guide
- Verified by Visa Operations and Dispute Resolution Guide
- Verified by Visa Artwork and Reproduction and Applications Guide

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. These publications and materials are designed to assist issuers, acquirers and merchants in the development and support of 3-D Secure capabilities. Some 3-D Secure documents are available only to parties that have executed a license agreement. To request a copy of the *Visa Authenticated Payment Program License Agreement* and licensed documents, send an email to 3DCompliance@visa.com.

3-D Secure Compliance and Testing Services

Issuers, acquirers, or merchants that build or buy 3-D Secure software will need to review the 3-D Secure compliance and testing publications. These documents require that the *Visa Authenticated Payment Program License Agreement* be completed. To obtain these license agreement and documents, please email Visa at: 3DCompliance@visa.com.

For More Information

More information about Verified by Visa or 3-D Secure is available through Visa Online at www.us.visaonline.com. Click the *Products and Services* tab, then, click on the “Verified by Visa” link.

Chapter 1 Introduction

Verified by Visa is a service that helps improve the security of online payment transactions. It is designed to assist in increasing cardholder and merchant confidence in online purchases, and reducing disputes and fraudulent activity related to the use of Visa payment cards.

Verified by Visa enables participating issuers to authenticate a cardholder during an online purchase. Authentication is the process of the issuer validating the card presenter's ownership of the Visa card account for payment online. The issuer verifies a cardholder's pre-established Verified by Visa password or identity information provided by the cardholder.

Cardholders can help to protect their Visa card account from unauthorized use by registering their existing account and establishing a Verified by Visa password with their card issuer.

Once activated, they can shop at any participating online merchant using that card account and password. Each time they shop online at a participating merchant, they should see a Verified by Visa window, where they authenticate themselves to their issuer. After verifying the cardholder's identity, the issuer creates and sends a Payer Authentication Response message to the merchant, providing the authentication result during the checkout process.

Upon receiving the issuer's Authentication Response, the merchant sends a Visa Authorization Request, including authentication data required for Verified by Visa transactions, to its acquirer. The transaction is completed through traditional payment processing through VisaNet via authorization, clearing and settlement.

With Verified by Visa, cardholders should have more confidence buying online. Verified by Visa helps to reduce the fraud exposure of issuers, acquirers, and merchants.

Business Objectives

The service objectives are highlighted in Table 1-1.

Table 1-1: Verified by Visa Objectives

Improve online purchases	• Enhance security and integrity of online purchase transactions. • Enable Issuers to authenticate cardholders for electronic commerce. • Uniquely identify online transactions.
Reduce operational expense	• Reduce operational expense and chargebacks related to unauthorized use of Visa cards for online purchases. • Link authentication with authorization and settlement transactions to ensure the data integrity of online transactions. • Provide proof for issuers, acquirers, and merchants of authentication, including attempted authentications. • Streamline dispute resolution processes through the use of automated tools to prevent invalid exception items.
Reduce risk associated with online transactions	• Ensure that issuers have the tools to approve online transactions with minimized exposure to fraudulent transactions. • Ensure that acquirers have the tools necessary to encourage the growth of online merchants and sales volume, with reduced exposure to fraudulent transactions. • Ensure that VisaNet has the capabilities to provide related online transaction processing support services to issuers.

The Three-Domain Model

Verified by Visa is based on the Three-Domain Secure (3-D Secure) Protocol, which uses Secure Socket Layer (SSL) encryption to collect and protect payment card information transmitted via the Internet. Verified by Visa defines three domains for the authentication process:

Issuer Domain – The issuer is responsible for determining whether authentication is available for the card account presented in an online purchase transaction.

Acquirer Domain – The acquirer accepts online transaction data from the merchant and passes it to Visa. The acquirer also ensures that its merchants originating online transactions are operating under a Merchant Agreement with the acquirer, in accordance with the business rules and technical requirements for the service.

Interoperability/Visa Domain – Operated by Visa, transactions are exchanged and stored using 3-D Secure as the common technology protocol.

Table 1-2 lists the three domains and their components.

Table 1-2: Components of the Verified by Visa Infrastructure

Domain	Component	Description
Issuer Domain	Issuer Enrollment Server	A server that manages cardholder activation by presenting a series of questions to be answered by the cardholder and verified by the issuer. The Enrollment Server is operated by the issuer or a third-party processor.
	Issuer Access Control Server (ACS)	A server with activated cardholder account and access information. The Access Control Server (ACS) is operated by the issuer or a third-party processor, called an ACS processor. It validates cardholder participation in the service; provides proof of authentication, including attempted authentications, and provides digitally signed responses to merchants.
Acquirer Domain	Merchant Plug-in (MPI)	A software module integrated into merchant website checkout processes, used to provide the interface between the Verified by Visa service and the merchant's payment processing software. The software also verifies issuers' digital signature used to sign authentication responses to the merchant.
Interoperability/ Visa Domain	Directory Server	A server operated by Visa to route authentication requests from merchants to issuer ACSs.
	Transaction Routing Service (TRS)	The Visa Transaction Routing Service transmits all Payer Authentication Requests from participating merchants to issuer ACSs to ensure a timely response to merchants.
	Visa Attempts Service	The Visa Attempts Service provides merchants with responses to attempted authentications for U.S. cardholders if the issuer or cardholder is not participating in Verified by Visa or the issuer ACS is not available.
	Authentication History Server (AHS)	A server operated by Visa that stores authentication transactions. The Authentication History database is used to verify authenticated transactions and to provide information during dispute resolution, if needed by an issuer or acquirer.
	VisaNet	The VisaNet system that processes authorization, clearing and settlement, including verification of the Cardholder Authentication Verification Value (CAVV) that is forwarded in the Visa Authorization Request.

Verified by Visa Symbol

Verified by Visa is the brand name that cardholders associate with their issuer's online authentication capability. Cardholders see the Verified by Visa Symbol while registering for the service and as part of the online authentication during each shopping experience.

Participating merchants use the Verified by Visa Symbol on their website to communicate to cardholders that they offer this enhanced security.

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 chip cards or cardholders who use chip cards.

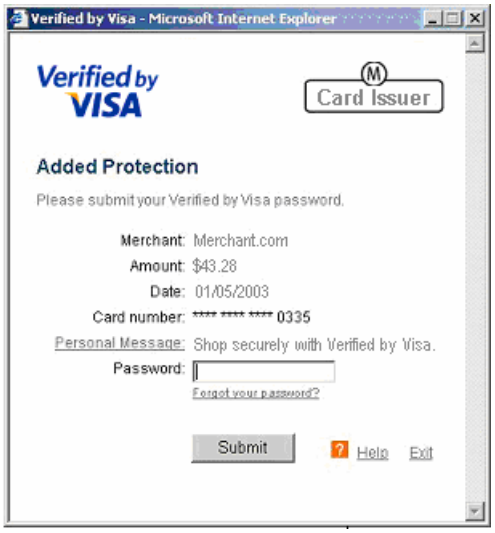
Cardholder Activation

Cardholder activation is the process in which a cardholder is authenticated by the issuer to ensure that he or she is entitled to register the card account. Verified by Visa enables real-time cardholder authentication by participating issuers. Online purchases are authenticated when the cardholder correctly enters the information requested by the issuer and the issuer ACS returns a Payer Authentication Response to the merchant.

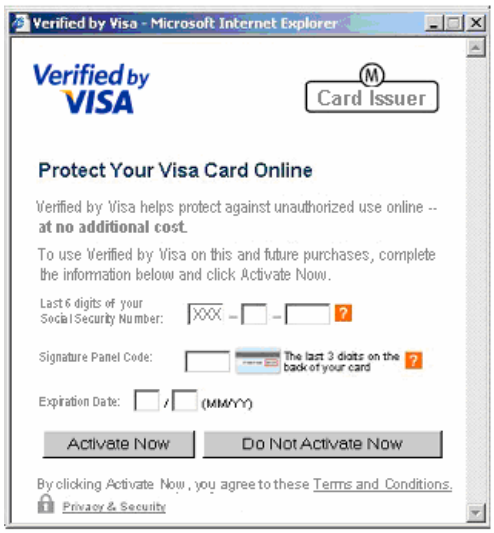
Cardholders may activate their Visa cards in a number of ways. They can visit the Verified by Visa site at Visa.com and be directed to their issuer's web site for enrollment. The issuer may also pre-enroll their cardholders to enable authentication and activation during a transaction.

Figure 1-1: Sample User Interface for Cardholder Activation

Cardholder Enters Personal Password



Cardholder Enters Authentication Data



Shown in Figure 1-1 above are sample user interface pages that cardholders may see from their issuers. All issuers and their Access Control Server Processors are required to adhere to the standards and requirements. After the cardholder selects the "buy" or "submit" button, the cardholder

is presented with a Verified by Visa page from the issuer's Access Control Server. On the left, the cardholder is authenticated by entering his/her personal password. On the right, the cardholder is authenticated by entering the data requested by the issuer and is activated for Verified by Visa.

In both cases, the issuer Access Control Server returns an Authentication Confirmation to the merchant. This response message includes the authentication data (the Electronic Commerce Indicator and Cardholder Authentication Verification Value) for submission with the Authorization Request.

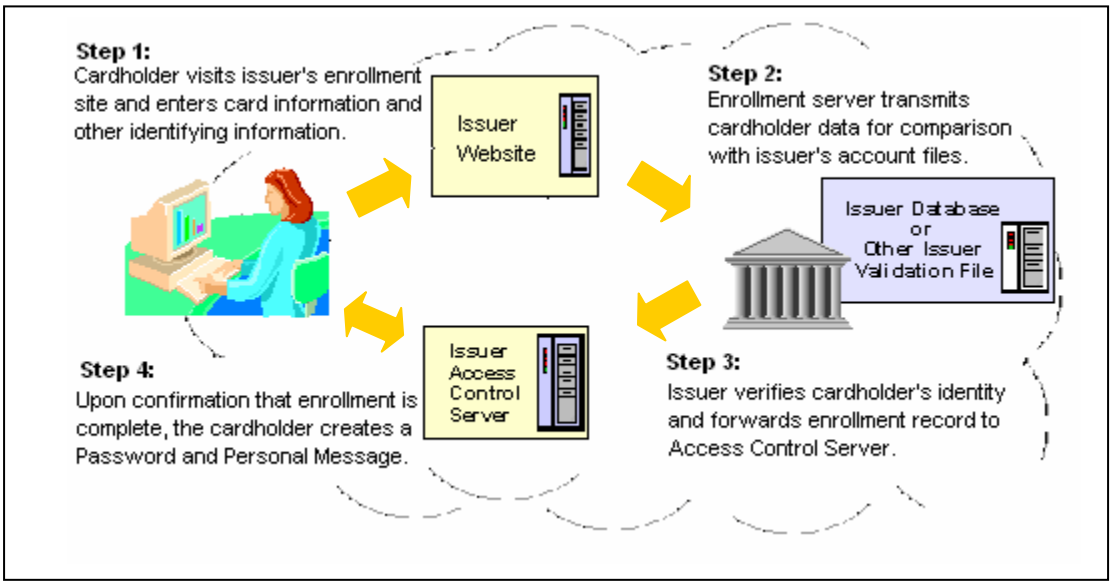
Issuer Enrollment Website

An individual cardholder may also be activated in response to issuer communications or advertising by visiting the issuer's website. The cardholder is asked for personal information that allows the issuer to complete cardholder authentication, for example, name, address, and other identity information. A cardholder may visit one of following:

- The issuer enrollment website, where the cardholder provides all required authentication information, and then selects a password and personal message.
- The issuer's online banking website, where the cardholder may opt to participate in Verified by Visa, agrees to use the existing online banking password, and selects a personal message.

At the issuer's option, the cardholder may be asked to provide a password hint or user ID, in addition to a password and personal message. Figure 1-2 illustrates the cardholder enrollment process.

Figure 1-2: Issuer Enrollment Website



When the cardholder initiates enrollment:

Step 1. The cardholder visits the issuer's enrollment website and enters authentication information.

Step 2. The issuer server transmits the cardholder information to the issuer database for verification.

Step 3. The issuer confirms the cardholder's identity and forwards an enrollment record to the Access Control Server to complete cardholder enrollment.

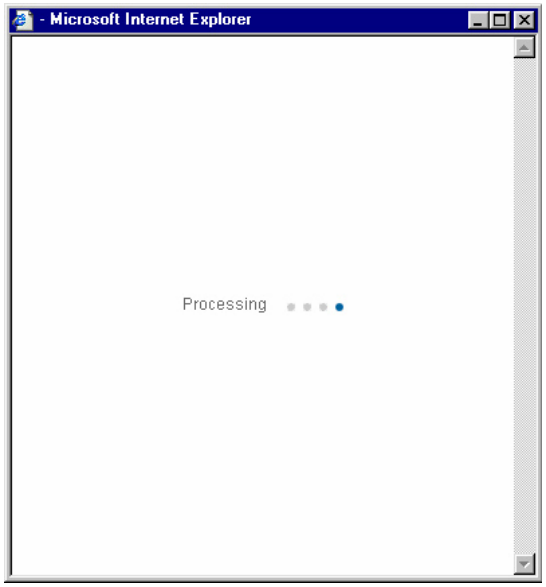
Step 4. The cardholder creates a Password and Personal Message.

Upon the completion of cardholder enrollment, cardholders will be asked for their Verified by Visa password when shopping at participating merchants.

Attempted Authentications

Some issuers may elect not to participate or some cardholders may not participate in Verified by Visa. To ensure that participating merchants are provided with the required proof of an attempted authentication, either the issuer Access Control Server or the Visa Attempts Service (for non-participating issuers and for stand-in processing if an Access Control Server is not operational) will return an Attempts Response. These transactions provide participating merchants with chargeback protection when the subsequent Authorization Request includes the required data. The customer experience for cardholders is shown in Figure 1-3.

Figure 1-3: Attempted Authentication Processing Page



Processing Page

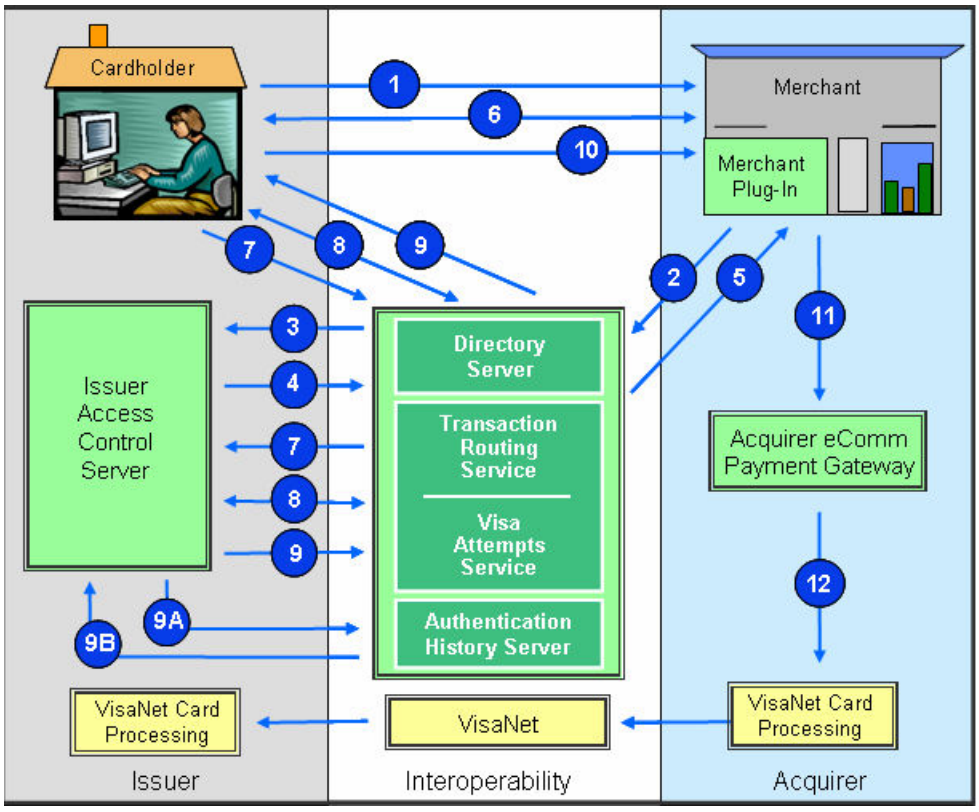
The processing for attempted authentications has no cardholder interaction. A "Processing" window (shown on the left) is briefly displayed while the Attempts Response is processed by the issuer Access Control Server or the Visa Attempts Service and returned to the merchant.

When the Verified by Visa merchant receives the Attempts Response, the message will have Electronic Commerce Indicator and Cardholder Authentication Verification Value for inclusion in the Authorization Request message. As noted earlier, these data elements must be included in the Authorization Request for the merchant to receive chargeback protection

Chapter 2 Transaction Flow

Once activated, the cardholder is authenticated during each online purchase at participating merchants. The cardholder visits a participating merchant online site, selects goods or services, and proceeds to the checkout page. There, the cardholder may complete the checkout information in one of a variety of ways – for example, self-entered, electronic wallet, or merchant one-click. The cardholder initiates a purchase transaction, as described below in Figure 1-4.

Figure 1-4: 3- D Secure Transaction Flow



Step 1. The cardholder completes the purchase by clicking the *Buy* or *Submit* button. This activates the Merchant Plug-In and initiates a Verified by Visa transaction.

Step 2. The Merchant Plug-In identifies the card account number and sends it to the Visa Directory Server to determine whether the card is in a participating card range.

Step 3. If the issuer is participating for the card range, the Visa Directory Server sends a Verify Enrollment Request message to the issuer Access Control Server, via the Visa Transaction Routing Service, to determine whether authentication is available for this card number.

Step 4. The Access Control Server returns a Verify Enrollment Response to the Visa Directory Server:

- If authentication is available for this card number, the response provides the URL of the Visa Transaction Routing Service and the Access Control Server where the cardholder can be authenticated or an attempted authentication will response will be generated.
- If authentication is not available, the merchant server receives a Cardholder Not Enrolled or Authentication Not Available message and returns the transaction to the merchant's commerce server to proceed with a standard transaction processing.

Step 5. The Visa Directory Server forwards the ACS response to the Merchant Plug-In.

Step 6. The Merchant Plug-In sends a Payer Authentication Request message to the cardholder's browser for routing to the Visa Transaction Routing Service and the issuer Access Control Server.

Step 7. The cardholder's browser passes the Payer Authentication Request to the Visa Transaction Routing Service which forwards the request to the Access Control Server.

Step 8. The issuer ACS authenticates the cardholder as described in the Cardholder Activation section. If the issuer is not participating in Verified by Visa, the Visa Attempts Service will return an attempted authentication response.

Step 9. The issuer ACS/Visa Attempts Service creates, digitally signs, and sends a Payer Authentication Response to the merchant via the Visa Transaction Routing Service and the cardholder's browser. The Payer Authentication Response includes the appropriate Electronic Commerce Indicator (ECI) and Cardholder Authentication Verification Value (CAVV) to provide the merchant with authentication data that will be inserted in the VisaNet Authorization Request message. The Access Control Server also sends transaction information to the Authentication History Server for storage.

Step 10. The cardholder's browser routes the Payer Authentication Response back to the Merchant Plug-In.

Step 11. The Merchant Plug-In validates the digital signature in the response, verifying that it is from a valid participating issuer. If the digital signature is verified and the issuer has sent an approved Payer Authentication Response, the cardholder is deemed authenticated and the Merchant Plug-In returns the transaction to the storefront software. The merchant starts processing the order, determining whether it can be fulfilled and calculating taxes and shipping for the total transaction amount.

If the merchant receives a failed authentication, the merchant should request another form of payment from the cardholder. Failed authentications are not permitted to be submitted for authorization.

Step 12. The merchant formats and sends to its acquirer a VisaNet Authorization Request message, which contains information from the issuer's Payer Authentication Response, including the CAVV and the ECI. The acquirer passes the Authorization Request to VisaNet and the transaction completes through standard VisaNet processing.

Chapter 3 Linking Authentication and Visa Processing

The Custom Payment Service Programs for electronic commerce transactions form the basis for identifying these transactions, establishing transaction business rules, and processing requirements.

Authentication Data in Authorizations

To provide issuers with a method to validate the results of an online cardholder authentication, the issuer Access Control Server creates a Cardholder Authentication Verification Value (CAVV). The CAVV is a cryptographic value derived by the Access Control Server, using encryption keys established for that issuer. The CAVV and Electronic Commerce Indicator (ECI) are included in the Payer Authentication Response message from the Access Control Server and are transmitted by the merchant to its acquirer for inclusion in the Visa Authorization Request. The issuer's Visa processor, or Visa on the issuer's behalf, uses the issuer's CAVV encryption keys to validate the CAVV. Cardholder Authentication Verification Values are generated both for cardholder authentications and attempted authentications.

Chargeback Protection for Verified by Visa Transactions

Cardholder Authentications

Participating Verified by Visa merchants enable issuers to authenticate their cardholders during online purchases; thus, potentially reducing the fraudulent use of Visa cards. When an issuer Access Control Server authenticates a cardholder and the merchant includes the designated authentication data (a CAVV when returned by the Access Control Server and ECI) in the Visa Authorization Request message, issuers are not permitted to charge back these transactions if the cardholder alleges that they did not participate in the online purchase.

Attempted Authentications

When merchants participating in Verified by Visa attempt to authenticate a Visa cardholder, but do not receive an authentication response because either the issuer or cardholder is not participating, the Verified by Visa program provides the merchant with chargeback protection for an attempted authentication. Issuers are not permitted to charge back Verified by Visa attempted authentications.

There are certain exclusions for which merchants retain chargeback liability when cardholders are either authenticated with Verified by Visa or there is an attempted Verified by Visa authentication. More information is available in the *Verified by Visa Operations and Dispute Resolution Guide*.

Chapter 4 Implementation Considerations

Issuers, acquirers, and merchants have a range of options for participating in Verified by Visa.

General Planning Considerations

Issuer Planning

Issuers need to consider the following:

- Develop identity authentication policies and cardholder authentication information to be used to verify the identity of cardholders.
- Determine where cardholder activation and Access Control Server functionality will be hosted. Issuers may support Verified by Visa directly or contract for these services with an Access Control Server processor.
- Establish the method(s) for cardholder activation.

Acquirer and Merchant Planning

Acquirers solicit and sign merchants for participation and must have a Merchant Agreement with each participating merchant covering 3-D Secure authentication for electronic commerce purchases. Online merchants install a Merchant Plug-in along with Visa-issued digital certificates to format transactions and facilitate their participation in the service.

For More Information

For more information on Verified by Visa, please visit Visa Online at www.us.visaonline.com to obtain a copy of the *Verified by Visa Acquirer and Merchant Implementation Guide* or the *Verified by Visa Issuer Implementation Guide*.