Visa Secure Program Guide

Visa Supplemental Requirements

Version 1.8

January 2025

Visa Confidential

Important Information on Confidentiality and Copyright

This document is a supplement of the *Visa Core Rules and Visa Product and Service Rules*. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the *Visa Core Rules and Visa Product and Service Rules*, the *Visa Core Rules and Visa Product and Service Rules* shall govern and control.

If you have technical questions or questions regarding a Visa service or capability, contact your Visa representative.

Contents

Tables

Figures

Summary of Changes

Version 1.8 Updates

Change	*Description*	*Section(s)*
Update	Updated the name of MCC 5967 from Direct Marketing-Inbound Teleservices to Adult Content and Services.	Section 2.5, Table 2-1
Update	Changed Visa Online (VOL) to Visa Access.	Throughout
Update	Updated attempts processing exclusions to accommodate standing-instruction MITs.	Section 2.7.2
Add	Added support of standing-instruction MIT authentication.	Section 2.8.3, 2.12.4
Add	Added the value of I (Informational only) to the list of transaction statuses for 3DS Server.	Section 1.3.5
Delete	Removed references to EMV 3DS 2.1, as the version is no longer supported.	Throughout

Version 1.7 Updates

Change	*Description*	*Section(s)*
Update	Changed “cardholder” to “cardholder account ID” to clarify authentication process.	Throughout
Delete	Deleted all mentions of 3DS 1.0.2	Throughout
Update	Updated Issuer Requirements for Visa Data Only	Section 2.18.1

Version 1.6 Updates

Change	*Description*	*Section(s)*
Add	Added VSS access information.	Introduction
Update	Changed "Visa Secure Data Only" to "Visa Data Only."	Sections 2.18, 2.18.1
Update	Updated Issuer Rules and Requirements.	Section 2.2
Update	Updated CAVV Not Present Restriction in Table 2–1: Merchant Dispute Protection Exceptions	Section 2.5.1
Add	Added CAVV Reuse and Storage section.	Section 1.3.2.1
Add	Added Visa Secure Smart Attempts information.	Section 2.7.1
Delete	Deleted Data Only from the list of Attempts Processing Exclusions.	Section 2.7.2
Update	Updated Browser Screen Width and Browser Screen Height Message Category: Payment to Required Conditional	Section A, Table A-4
Delete	Deleted Browser Screen Width and Browser Screen Height from list of browser transactions in data quality monitoring sections	Section A

Version 1.5 Updates

Change	*Description*	*Section(s)*
Add	Added Visa Secure Issuer requirements update effective 12 April 2025 for Canada regarding authentication.	Section B.1
Update	Updated date of 12 April 2024 to 13 May 2024 for Visa Secure Issuer requirements regarding mandate to support EMV 3DS 2.2.0.	Section 2.2
Add	Added activation and auto-enrollment of Canadian issuers into the 3DS Digital Authentication Framework on Visa Secure.	Sections 2.16, 2.16.1, 2.16.2 2.16.3

Version 1.4 Updates

Change	*Description*	*Section(s)*
Add	Added Visa Secure On-Behalf-Of Issuer Services information.	Section 2.17
Add	Added Visa Method URL information	Sections 1.2.4.1, 2.12.1
Add	Visa Data Only program requirements	Section 2.18
Add	Additional of program mandates effective 12 August 2024 for authentication data quality requirements.	Sections A, A.1

Version 1.3 Updates

Change	*Description*	*Section(s)*
Add	Acquirer / Merchant requirement to send authentication requests to the highest protocol supported by the Issuing range.	Section 2.3
Add	Added transaction status reason codes related to FIDO.	Table 1.5

Version 1.2 Updates

Change	*Description*	*Section(s)*
Update	Updates made to the authorization processing section.	Section 2.10
Edit	Amended the Authorization Performance Thresholds for DAF formulas.	Section 2.16.3
Add	Added references to the twelve additional data fields required for EMV 3DS authentication requests.	Section A

Version 1.12 Updates

Change	*Description*	*Section(s)*
Update	Updated the reference to 1.0.2 compliance testing requirements.	Section 2.1

Introduction

The *Visa Secure Program Guide* contains information about:

- Visa Secure
- Program Rules

This document is a supplement of the *Visa Core Rules and Visa Product and Service Rules.* In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the *Visa Core Rules and Visa Product and Service Rules*, the *Visa Core Rules and Visa Product and Service Rules* shall govern and control.

Audience

This Guide is a global guide intended for Issuers who are:

- Evaluating Visa Secure Program OR
- Planning a Visa Secure Program implementation

Scope

This document is for **Visa Secure** and its use to support authentication of payment transactions.

EMV 3DS—EMVCo began work in 2015 to advance 3DS through its open specifications creation process. The focus of EMV 3DS is to enhance the protocol in the areas of authentication, user experience, technology, performance, security, and flexibility to promote the longevity of the protocol for the benefit of Visa Secure as well as the other payment systems. EMVCo is the owner of EMV 3DS.

Table 2: EMV 3DS Protocol Version Numbers

Protocol Version Numbers	Status
2.0.0	Deprecated
2.1.0	Deprecated
2.2.0	Active
2.3.0	Active (Currently not supported by Visa)

References

The following references are available to support a Visa Secure implementation.

Visa

Visa references can be accessed through Visa Access, unless otherwise noted.

- **Brand Standards**—Visa's Master Brand, artwork, reproduction, and application guidelines can be accessed through Visa Access or at www.productbrandstandards.com
- **CAVV Technical Details—** *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.
- **Digital Certificates**—Contact your Visa regional representative for details. Forms and procedures vary by region.
- **Dispute Resolution**—*Visa Secure Dispute Resolution Guide*
- **Implementation Guides**
  - *Visa Secure - Issuer Implementation Guide for EMV 3-D Secure*
  - *Visa Secure - Merchant/Acquirer Implementation Guide for EMV 3-D Secure*
- **Visa Rules**—*Visa Core Rules and Visa Product and Service Rules* (referred to as the "Visa Rules")
- **PSD2 SCA for Remote Electronic Transaction Implementation Guide**—*Set of Visa guidance documents that are relevant to the implementation of Strong Customer Authentication under PSD2*
- **Implementing Strong Consumer Authentication (SCA) for Travel & Hospitality**—*Guide to explain how to implement SCA solutions in the travel and hospitality sector*
- **Digital Authentication Framework (DAF)—** *Digital Authentication Framework 3-D Secure Implementation Guide for Merchants / Acquirers*

EMVCo

EMV 3DS specifications can be found on EMVCo's website and include the following:

- **3DS Specification**—*EMV® 3-D Secure Protocol and Core Functions Specification*
- **3DS SDK Reference**—*EMV® 3-D Secure SDK Specification*
- **3DS SDK Reference**—*EMV® 3-D Secure Split—SDK Specification*
- **3DS SDK Reference**—*EMV® 3-D Secure SDK—Device Information*
- **3DS SDK Reference**—*EMV® 3-D Secure SDK—Technical Guide*

Industry Standards

- **Data Security**

- *Payment Card Industry Data Security Standards (PCI DSS)*—PCI DSS security requirements applicable to third party ACS, DS, and 3DS Server service providers (https://www.pcisecuritystandards.org/security_standards/documents.php). Filter by PCI DSS
- *Payment Card Industry (PCI) 3DS Security Requirements and Assessment Procedures for EMV®*—PCI 3DS security requirements applicable to third party ACS service providers (https://www.pcisecuritystandards.org/security_standards/documents.php). Filter by 3DS

Other Resources

Other implementation resources include:

Visa Access

Visa Access is a business-to-business extranet that provides secure access to important Visa content and services for our clients around the world. Visa Access is available to enrolled clients, approved third-party partners, Visa employees, contractors, agencies, and vendors.

- Information about Visa Secure can be found by selecting "Visa Secure" under "Risk" in the top navigation bar from the Visa Access home page.
- A Visa Access user ID and password is required to access Visa Access. Please contact your Visa representative to request access.

Visa Secure Services (VSS)

VSS is a service available through Visa Access that provides clients access to Visa Secure information and subscription-based services. There is no fee for the use of VSS.

VSS can be accessed at www.visasecureservices.com. For more information about VSS, see Requesting Access to Visa Secure Services.

Contact Information

The following contacts are available to answer any additional questions regarding:

- **Visa Secure Program**

  Visa regional support teams are available to answer your questions about Visa Secure. Contact the team for your region using the email address below:
  - North America: esupport@visa.com
  - Latin America, and Caribbean (LAC): Visa Support Hub (VSH) in Visa Access.

  - Asia Pacific (AP): isupport@visa.com
  - Central Europe, Middle East, and Africa (CEMEA): csupport@visa.com
  - European Region: customersupport@visa.com
- **Visa Rules**
  - Email: visarulesinquiries@visa.com

1 Visa Secure Program

This chapter provides an overview of Visa Secure and includes:

- **Introduction**—Describes Visa Secure purpose, the 3-D Secure Protocol, and the benefits of the program.
- **How Visa Secure Works**—Provides a high-level overview of the Visa Secure transaction flow along with information on the associated participants and components.
- **Visa's Authentication Data**—Highlights the key data elements associated with Visa Secure: Electronic Commerce Indicator (ECI), Cardholder Authentication Verification Value (CAVV), CAVV Results Code, and the 3-D Secure Indicator.
- **Message Details and Transaction Flows**—Outlines the Visa Secure messages along with the Frictionless flow, the Challenge flow (for both browser use and merchant application use), and the authorization flow.

1.1 Introduction

Visa Secure is a global solution designed to make e-commerce transactions more secure by helping to ensure the transaction is initiated by the rightful owner of the Visa account. Implementing Visa Secure can improve profitability through increased sales and reduced operational costs.

The Three-Domain Secure (3-D Secure or 3DS) Protocol that Visa Secure is based on serves as the mechanism for cardholder authentication at the time of an e-commerce purchase. For merchants and issuers, Visa Secure provides an additional layer of security prior to authorization, and for cardholders, it creates the trust they seek when shopping online.

1.1.1 Authentication vs. Authorization

Visa Secure focuses on cardholder authentication for e-commerce transactions. Authentication and authorization are distinctly different processes with different business objectives:

- **Authentication** is the process of helping to ensure that the cardholder is the rightful owner of the Visa payment account. Authentication takes place using the issuer's selected authentication method. See the next section for more information.
- **Authorization** is the process used by a card issuer to approve or decline a Visa payment transaction from a merchant/acquirer or other card acceptor.

Authentication using Visa Secure, if invoked by the merchant, occurs before authorization and outside of the authorization stream. Once authentication is completed, then authorization may occur through the merchant's acquirer following the standard process.

1.1.2 Authentication Methods

Depending on the authentication solution the Issuer chooses, there are many authentication methods available for an issuer to use.

Visa recommends that issuers use risk-based authentication as their authentication approach, when appropriate—recognizing that in some cases regulatory requirements may have specific "step-up" or challenge authentication requirements. With risk-based authentication, the issuer will assess the risk of the transaction and then either:

- Complete authentication without involving the cardholder. OR
- If needed, request further authentication by challenging the cardholder through a dynamic method[1].

Risk-based authentication typically results in a frictionless experience for the cardholder and limits cardholder involvement in the authentication process to those transactions that require additional verification.

If additional verification of the cardholder is required, Visa recommends that a dynamic (rather than static) method be used. A dynamic authentication method is one where the data entered by the cardholder is different for each transaction—the information entered is only valid for one transaction and can be entered into the authentication screen to verify the cardholder's identity. A one-time passcode is an example of a dynamic authentication method.

Visa Secure-specific static passwords are not allowed as an authentication method.

1.1.3 Benefits

Visa Secure involves cardholders, issuers, merchants, acquirers, and Visa. Visa Secure is designed to benefit all participants in an e-commerce payment transaction. The benefits include:

- Optimized Approvals—Used as another layer of fraud defense, false-positives can be minimized allowing increased authorization throughput.
- Reduced Operational Expenses—A decrease in fraudulent disputes and their associated losses and processing costs contribute to a healthier bottom line.
- Increased Consumer Confidence—The use of more robust authentication methods at the time of purchase improves security and reduces friction, which in turn bolsters consumer confidence leading to increased profitability for merchants and issuers.

[1] In some cases, an active challenge of the cardholder may be required due to local/country regulations.

1.1.4 Participants

The main participants in a Visa Secure transaction are described in the table below.

Table 1–1: Participants in a Visa Secure transaction

Participants	Roles
Cardholder	• Uses Visa card to pay for online purchases from a merchant's website or merchant's e-commerce application (which resides on a device such as a smart phone) • Is authenticated according to issuer's choice of authentication method
Issuer	• Manages the issuer's authentication program according to the Visa Secure guidelines • Uses software to authenticate the cardholder account ID during online purchases; this software is referred to as the Issuer Access Control Server (ACS) • Provides a cryptographic value for each authenticated transaction; this value is called a Cardholder Authentication Verification Value (CAVV) • Receives VisaNet authorization messages from acquirers, which includes Visa Authentication Data, and responds with authorization decisions See *Section 1.3: Visa Authentication Data* for details.
Merchant	• Offers merchandise or services at an e-commerce website or via merchant's e-commerce application and accepts Visa for payment • Uses software to support Visa Secure Program; this software is referred to as the 3DS Server and optionally a 3DS Software Development Kit (SDK) • Sends Visa's Authentication Data to the acquirer as part of the authorization message
Acquirer	• Signs up merchants to participate in Visa Secure • Ensures that merchants originating e-commerce transactions are operating under a Merchant Agreement with the acquirer in accordance with the business rules and technical requirements of Visa Secure • Receives transaction details from merchants, including Visa Authentication Data to include in the authorization, formats and submits authorization messages to issuers through Visa; and provides the issuer's authorization decision to merchants • Responsible for signing up 3DS Server providers as third-party agents
Visa	• Operates components of the Interoperability Domain for Visa Secure, including the Visa Secure Directory Server and Visa's Attempts Service • Operates VisaNet to route payment transactions between issuers and acquirers • Offers issuer services where VisaNet can verify the CAVV on the issuer's behalf for all transactions or those processed in VisaNet Stand-in • Manages Visa 3DS Security Program that ensures third parties performing ACS or DS services on behalf of issuers comply with applicable requirements

1.2 How Visa Secure Works

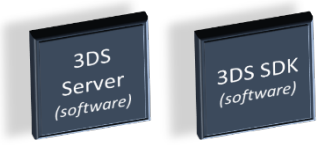
This section provides an overview of Visa Secure including:

- Domains and Components Overview
- Merchant/Acquirer Domain
- Issuer Domain
- Visa Interoperability Domain
- Transaction Flow Overview
- Dispute Requirements

1.2.1 Domains and Components

Visa Secure defines three distinct domains that interact to support authentication and authorization a Merchant/Acquirer Domain, the Visa Interoperability Domain, and Issuer Domain.

Figure 1-1: Domains and Components

Merchant / Acquirer Domain	Visa Interoperability Domain	Issuer Domain
 3DS Server / 3DS SDK	 Visa Secure Directory Server	 Issuer Access Control Server (ACS)
 Merchant's E-Commerce Software	 Visa Secure Attempts Service	
 Acquirer / Acquirer Processor	 VisaNet	 Issuer / Issuer Processor Host System

1.2.2 Merchant/Acquirer Domain

The Merchant/Acquirer Domain includes Merchant's e-commerce checkout, Authentication, and Authorization components.

1.2.2.1 Merchant's E-Commerce Checkout Environment

Merchants can invoke Visa Secure for consumers shopping on the Merchant's e-commerce websites using a browser or shopping via the merchant's e-commerce application on a device (e.g., mobile application or mobile browser).

1.2.2.2 Authentication Components

A merchant's authentication components enable the merchant to send and Visa Secure messages and include:

- 3DS Server software to enables the merchant to use 3DS authentication with consumers using browser-based devices
- 3DS Software Development Kit (SDK) software enables the merchant to use 3DS with consumers using device-based applications (e.g., a mobile application)

1.2.2.3 Authorization Components

A merchant's authorization components enable the merchant to interface with VisaNet to process payment transactions. A merchant's authorization components generally include:

- Payment Processing System—Software that creates and sends the payment transaction information to the acquirer processor, including Visa Authentication Data that is sent to the Issuer in the authorization message.
- Acquirer Processor—The acquirer host system that communicates with VisaNet to process payment transactions.

1.2.3 Issuer Domain

The Issuer Domain includes Authentication and Authorization components.

1.2.3.1 Authentication Component

Issuer ACS—The Issuer ACS responds to authentication requests and performs cardholder account ID authentication.

- The issuer defines the authentication methods and the criteria that the ACS uses to determine what type of authentication is needed.
- The Issuer's ACS creates the CAVV and provides it to the merchant in the authentication response.
- The merchant includes the CAVV in the authorization request message to the issuer as proof that authentication was performed.

1.2.3.2 Authorization Component

Issuer Host—The Issuer Host system communicates with VisaNet to process payment transactions.

- The Issuer Host receives the VisaNet authorization message and uses Visa Authentication Data included in the transaction to approve or decline the purchase.
- The Visa Authentication Data in the authorization message includes the CAVV. The issuer can use the CAVV to support the authorization decision process.
- Visa Secure requires the Issuer verify the CAVV sent in the authorization request by the Merchant/Acquirer. VisaNet offers a service where VisaNet can perform CAVV verification on behalf of the Issuer.

1.2.4 Visa Domain

The Visa Domain, also referred to as the Interoperability Domain, includes Authentication and Authorization components.

1.2.4.1 Authentication Components

Visa operates Visa Secure Directory Server, the Visa Secure Attempts Service, and the Visa Method URL

- Visa Secure Directory Server—The Visa Secure Directory Server routes Visa Secure messages between 3DS Servers and the Issuer ACS.
- Visa Secure Attempts Service—Is a Visa service that responds to authentication request messages on behalf of the Issuer when either the Issuer does not participate in Visa Secure or the Issuer participates but their ACS is unavailable. The Visa Secure Attempts Service provides proof, in the form of a CAVV, in the authentication response that the merchant attempted to obtain authentication.
- Visa Method URL — is a 3DS Method URL capability provided by Visa on behalf of Issuers. When the Visa Method URL is present for a card range, it is invoked by 3DS Requestors for browser authentication transactions as defined in the EMV 3-D Secure specification, and allows for the capture of additional browser and device information to help facilitate transaction risk assessment.

1.2.4.2 Authorization Components

Visa's authorization component is VisaNet and VisaNet's CAVV verification service.

- VisaNet—Is a collection of systems and services where Visa offers online financial processing, authorization, clearing, and settlement services to issuers and acquirers.
- CAVV Verification— VisaNet can perform CAVV verification on behalf of the issuer during authorization processing OR during Visa Stand-In Processing (STIP) when the Issuer's Host is not available). The issuer must provide their CAVV keys to VisaNet to participate in these services.

1.2.5 Dispute Requirements

When Visa Secure authentication is successful or attempted authentication is completed for a transaction, the Merchant is protected against e-commerce fraud-related disputes.

The Merchant must include the CAVV received during authentication in the authorization request for every Visa Secure transaction.

1.3 Visa Authentication Data

Visa Authentication Data is used to communicate information about authentication between the Issuer ACS, the Merchant, VisaNet, and the Issuer Host.

The Merchant receives some Visa Authentication Data from the Issuer ACS during authentication. Visa Secure requires that this data be sent in the authorization request to VisaNet and the Issuer. Authentication Data created during authentication by the Issuer ACS, or Visa's Attempts Service include:

- Electronic Commerce Indicator (ECI)
- Cardholder Authentication Verification Value (CAVV)

Other Visa Authentication Data are created by VisaNet or the Issuer (in one scenario only) during authorization; these fields include:

- 3-D Secure Indicator (3DS Indicator)
- CAVV Results Code (created by the Issuer or VisaNet)

For information about Visa Authentication Data requirements, see Appendix A, Visa Secure with EMV 3DS Minimum Data Requirements.

1.3.1 Electronic Commerce Indicator (ECI)

The Issuer ACS or an Attempts Server provides the ECI value to the Merchant during authentication. The ECI indicates the level of authentication that was performed on the transaction.

The Merchant must include the ECI value received from authentication in the authorization request. Visa's ECI values are shown in the table below.

Table 1–2: Electronic Commerce Indicator (ECI) Values

ECI Value	Description
05	Cardholder account ID authentication successful
06	Merchant attempted to authenticate the cardholder account ID
07	Non-authenticated e-commerce transaction

1.3.2 Cardholder Authentication Verification Value (CAVV)

The Issuer' ACS returns a CAVV in the authentication response message to the Merchant.

- The Issuer ACS creates a CAVV when cardholder account ID is fully authenticated; the corresponding ECI is 05

Visa Secure Attempts server creates a CAVV when the merchant attempted to authenticate the cardholder account ID.

- Visa Secure Attempts Service creates a CAVV when authentication is attempted; the corresponding ECI is 06 (or 05 for activated issuers on transactions that qualify for Smart Attempts)

Effective 17 October 2020 in the Canada Region, Europe Region, LAC Region, US Region. **Effective 17 April 2020** in the AP Region, CEMEA Region. CAVV usage 3 version 7 must be used when responding to Visa Secure EMV 3DS transactions.

A CAVV is unique for each authentication transaction. The CAVV provides proof that cardholder account ID authentication occurred or that the Merchant attempted authentication.

The Merchant/Acquirer must include the CAVV in the authorization request message.

1.3.2.1 CAVV Reuse and Storage

If authentication and authorization (containing a CAVV) are completed successfully, merchants/acquirers/3DSSs must not store or re-use CAVVs.

If not completed successfully, CAVVs can be reused if authorization resubmission is permitted per the guidance in the Visa Product and Service rule #0030640. In these cases, storage of CAVVs is also permitted for the length of time specified in the rule. If authorization resubmission is not permitted

per the Visa Product and Service rules it is required for a new CAVV to be requested and the prior CAVV should not be stored or reused by the merchant/acquirer/3DSS.

Note: Exceptions to CAVV reuse are permitted for a limited set of use cases in Europe. See VBN 13979 for more information. This CAVV reuse waiver will expire on 18 October 2024. If the transaction is a 1A decline (Additional customer authentication required [Europe Region only]), the merchant must resubmit the transaction and include a CAVV. If an unused CAVV is not available for the transaction, the merchant must submit an authentication request to obtain a new CAVV. For additional information, see "SCA Related Requirements for Electronic Commerce Transactions - European Economic Area, United Kingdom and CEMEA Countries Subject to SCA Requirements."

1.3.3 CAVV Results Code

The CAVV Results Code field contains results of CAVV verification performed during authorization:

- VisaNet will update the CAVV Results Code field with the CAVV verification results (e.g., PASS/FAIL), if the Issuer has opted for VisaNet to perform CAVV verification,
- The Issuer is responsible for updating the CAVV Results Code field with the CAVV verification results (e.g., PASS/FAIL), if the Issuer has opted to perform CAVV verification,

The CAVV Results Code communicates CAVV verification results (e.g., PASS/FAIL) and the value returned will also indicate if the CAVV was created by the Issuer's ACS, the Issuer's Attempts Server, or Visa's Attempts Service.

See *Appendix C: CAVV Verification Results Code (Field 44.13)* for more details.

1.3.4 3-D Secure Indicator (3DS Indicator)—Optional

The 3DS Indicator communicates the 3DS version number and the EMV 3DS authentication method used to authenticate the cardholder account ID. The 3DS Indicator can be used for authorization processing or for back-office activities (e.g., reporting or analytics).

The 3DS Indicator is a field that the Issuer or Acquirer can optionally choose to receive in authorization:

- The Issuer receives the 3DS Indicator in the authorization request message
- The Acquirer receives the 3DS Indicator in the authorization response message

Note: See *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*, *Visa Secure Merchant/Acquirer Implementation Guide*, or *Visa Secure Issuer Implementation Guide* for a list of 3DS Indicator values.

1.3.5 EMV 3DS Authentication Messages Descriptions and Transaction Status Values

This section provides a description of each message along with the response data (Transaction Status values, ECI values, and whether or not a CAVV is present).

Table 1–3: EMV 3DS Transaction Flow Messages and Transaction Status

Message Type				
Message	**Transaction Status**	**Transaction Status Description**	**ECI**	**CAVV**
Authentication Request /Response (AReq/ARes) The 3DS Server[2] sends the AReq through the Visa DS to the Issuer ACS or Attempts ACS Upon receipt, the Issuer ACS or Attempts ACS performs risk-based authentication and provides the results of authentication to the 3DS Server in the ARes	Y[3]	Authentication Successful	05	CAVV Present
	A[3,4]	Attempts Processing Performed Effective **23 April 2022**, issuers are not allowed to respond with this transaction status	06	
	I	Informational Only; 3DS Requestor challenge preference acknowledged.	07	CAVV Present
	N	Authentication Failed; Not Authenticated; Transaction Denied	07	No CAVV
	U[5]	Authentication Could Not Be Performed; Technical or Other Problem		
	R	Authentication Rejected		
	C[3]	Challenge Required to authenticate the cardholder account ID	Send a Challenge Request (CReq)	

[2] A server or system that the merchant (or third party on the merchant's behalf) uses to support Visa Secure program authentication processing.
[3] Not a valid response for an AReq sent with a 3DS Requestor Challenge Indicator 06 = No challenge requested (Data share only)
[4] NPA are excluded from Attempts Processing
[5] The Visa Attempts Server will stand in if an ARes = U is returned

Message Type				
Message	**Transaction Status**	**Transaction Status Description**	**ECI**	**CAVV**
	D	Challenge Required; Decoupled Authentication confirmed		
Challenge Request/Response (CReq/CRes) The 3DS Server (or 3DS SDK) sends the CReq to the Issuer ACS Upon receipt, the Issuer ACS challenges the cardholder through an authentication method such as OTP and responds to the 3DS Server or 3DS SDK with the CRes	Y	Authentication Successful	Results of the challenge are sent in the Results Request (RReq) message by the ACS to the 3DS Server.	
	N	Not Authenticated; Transaction Denied		
Results Request/Response (RReq/RRes) The Issuer ACS sends the RReq to the 3DS Server to provide the results of the challenge authentication The 3DS Server acknowledges the RReq by responding with the RRes	Y	Authentication Successful	05	CAVV Present
	N	Authentication Failed; Not Authenticated; Transaction Denied	07	No CAVV
	U	Authentication Could Not Be Performed; Technical or Other Problem		
	R	Authentication Rejected		

Exceptions

- ERROR RECEIVED—If the 3DS Server receives an error message the merchant may proceed with authorization with an ECI = 07 (non-authenticated e-commerce transaction).

  Note: This does not apply in countries where authentication is mandated.

- NOT AVAILABLE—If an Issuer ACS is not available, the Visa Secure Attempts Service will respond to the 3DS Server with ARes = A (Attempts Processing Performed), an Authentication Attempted ECI value, and a CAVV.

  The merchant may proceed to authorization and must provide the ECI value and the CAVV in the authorization message.

- **3DS Server**
  - Evaluates the ARes and RReq message and the Transaction Status provided by Issuer ACS/Attempts Server.
    - **Y**, **N**, **U**, **I**, or **A**, the merchant can proceed to authorization using the ECI value and CAVV (CAVV is only applicable for Y, A, or I (for Visa Data Only transactions)) provided by the Issuer ACS/Attempts Server.
    - **R**, it is not recommended to proceed to authorization.
    - **C**, **D** the frictionless flow transitions to the Challenge flow.
  - See *Table 1–4: EMV 3DS Transaction Flow Messages and* Transaction Status for Transaction Status details.
- **ACS**
  - If ACS responds ARes or RReq N, U, or R, a Transaction Status Reason Code should be included.
  - See *Table 1–4: EMV 3DS Transaction Flow Messages and Transaction Status Reason Code* for Transaction Status Reason Code details.

Table 1–4: EMV 3DS Transaction Status Reason Code

Message Type					
Message	**Transaction Status**	**Transaction Status Reason Code**	**Transaction Status Reason**	**ECI**	**CAVV**
Authentication Request /Response (AReq/ARes)	N U R	01	Card Authentication Failed	07	No CAVV
		02	Unknown Device		
		03	Unsupported Device		
		04	Exceeds authentication Frequency Limit		
		05	Expired Card		
		06	Invalid Card Number		
		07	Invalid Transaction		
		08	No Card Record		
		09	Security Failure		
		10	Stolen Card		
		11	Suspected Fraud		

Message Type					
Message	Transaction Status	Transaction Status Reason Code	Transaction Status Reason	ECI	CAVV
		12[6]	Transaction Not Permitted to Cardholder		
		13[7]	Cardholder not enrolled in service		
		14	Transaction timed out at the ACS		
		15	Low confidence		
		16	Medium Confidence		
		17	High Confidence		
		18	Very High Confidence		
		19	ACS Maximum Challenges		
		22	ACS technical issue		
		23	Decoupled Authentication Required by ACS but not requested by 3DS Requestor		
		24	3DS Requestor Decoupled Max Expiry Time Exceeded		
		25	Decoupled Authentication was provided insufficient time to authenticate cardholder account ID. ACS will not make attempt		
		26	Authentication attempted but not performed by the cardholder		
		20	Non-Payment transactions not Supported **Reason Code Not Allowed**	N/A	

[6] Issuer response when a merchant sends an Authentication Request with a 3RI Indicator not supported by Visa.
[7] The Visa Attempts Server will stand in if an ARes = N and Transaction Status = 13 is returned by the ACS

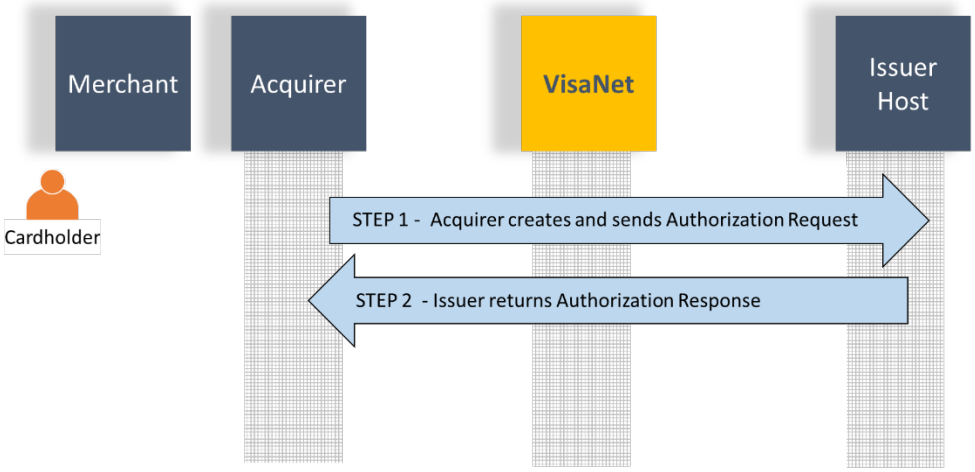
Message Type					
Message	Transaction Status	Transaction Status Reason Code	Transaction Status Reason	ECI	CAVV
		21	3RI transaction not supported **Reason Code not Allowed**		
		80[8]	Error Connecting to ACS	07	No CAVV
		81[8]	ACS Timed Out		
		82[8]	Invalid Response from ACS		
		83[8]	System Error Response from ACS		
		84[8]	Internal Error While Generating CAVV		
		85[8]	VMID not eligible for requested program		
		86[8]	Protocol Version Not Supported by ACS		
		87[8]	Transaction is excluded from Attempts Processing (includes non-reloadable pre-paid cards and Non-Payments (NPA))		
		88[8]	Requested program not supported by the ACS		
		89	CAVV is included in response	07	CAVV
		90[9]	Issuer SCA Required	07	No CAVV
		91[10]	Transaction can be used for a future FIDO enrollment	05	CAVV
		92[10]	Transaction cannot be used for a future FIDO enrollment	05	CAVV

[8] Visa Secure Directory Server (DS) Response only
[9] Europe Issuer response only for the DAF program. For more information refer to the DAF 3DS implementation guide.
[10] The '91'/'92' values in the RReq are only valid when the "3DS Requestor Authentication Information" was present and the "3DS requestor Authentication method" = '80' in the AReq. In the RReq, these values are only valid when the transaction is successful (Y/05/CAVV).

1.4 Authorization Overview

Once authentication is completed, the Merchant/Acquirer can submit the Visa Authentication data (i.e., ECI and CAVV) in the authorization request message to VisaNet and the Issuer.

Figure 1-2: Authorization Flow



1.4.1 Precursor to the Authorization Flow

The merchant provides the authentication results including the ECI value and the CAVV to their Acquirer/Acquirer Processor. The ECI and CAVV are provided to the merchant in the

- EMV 3DS
  - ARes message for a Frictionless Flow or
  - RReq message for a Challenge Flow

1.4.2 Authorization Flow (Authorization Request message)

- **Acquirer/Acquirer Processor:**
  - Creates the authorization request including the ECI and CAVV
  - Forwards the authorization request to the issuer through VisaNet
- **VisaNet**
  - Recognizes ECI 05 and 06 transactions as Visa Secure transaction:

  - If the Issuer has selected Visa to perform CAVV verification, VisaNet will verify the CAVV and provide the issuer with the CAVV verification results
  - If the Issuer has opted perform CAVV verification, VisaNet will forward the CAVV to the Issuer for the Issuer to verify
- Includes the 3DS Indicator to the Issuer in the authorization request, if the Issuer has elected to receive the 3DS Indicator.
  - The 3DS Indicator identifies the EMV 3DS protocol version and authentication method used during authentication.
- Includes the 3DS Protocol Version Number to the Acquirer in the authorization request, if the Acquirer has elected to receive the 3DS Protocol Version Number.
  - The 3DS Protocol Version Number identifies the EMV 3DS protocol version used during authentication.
- Forwards the authorization request to the Issuer Host for processing

1.4.3 Authorization Flow (Authorization Response message)

- **Issuer Host**
- Receives the ECI, CAVV, and CAVV Results (if signed up for the CAVV Verification Service) in the authorization message
- Verifies the CAVV and updates the CAVV Results field (if the issuer performs their own CAVV verification)
- Completes their authorization decision
- Returns the authorization response (approve or decline) to the acquirer via VisaNet.
- **VisaNet**
- Includes the 3DS Indicator to the Acquirer in the authorization request, if the Acquirer has elected to receive the 3DS Indicator.
  - The 3DS Indicator identifies the EMV 3DS protocol version and authentication method used during authentication.
- Includes the 3DS Protocol Version Number to the Acquirer in the authorization request, if the Acquirer has elected to receive the 3DS Protocol Version Number.
  - The 3DS Protocol Version Number identifies the EMV 3DS protocol version used during authentication.
- Forwards the authorization response to the Acquirer for processing
- **Acquirer/Acquirer Processor**
- Forwards authorization decision to the merchant.
- **Note:** For dual message endpoints, merchants/acquirers must ensure that the same ECI and CAVV values used in authorization messages are submitted in Clearing and Settlement messages.

- **Merchant**
  - Provides authorization response to cardholder.

2 Visa Secure Program Rules

This chapter outlines Visa Secure program rules:

- Visa Secure Program Participation Rules
- Issuer Rules and Requirements
- Acquirer Rules and Requirements
- Card Product Type Restrictions (Non-Reloadable Prepaid Cards)
- Dispute Protection and Exceptions
- CAVV Mandate
- Global Attempts Processing
- Use of Authentication Data in Authorization
- ECI 6 Decline Compliance Program
- Authorization Processing
- Authentication Approval Rates (U.S. Only)
- EMV 3DS Requirements
- Country Rules
- User Interface Requirements

2.1 Visa Secure Program Participation Rules

A Visa Secure participant must:

- Complete Visa Secure program enrollment process.[11]
- Ensure that its Visa Secure for EMV 3DS component[12] has successfully met the requirements of the EMVCo 3-D Secure Compliance Testing Program and Visa Secure Product Certification Testing.
- Only use a digital certificate issued by or associated with Visa as an authentication mechanism for a Visa product or service.

[11] See *Issuer or Merchant/Acquirer Implementation Guide*
[12] ACS for issuers and 3DS Server and/or 3DS SDK for merchants/acquirers.

- Adhere to the EMVCo 3-D Secure data inclusion requirements[13].

2.2 Issuer Rules and Requirements

A Visa Secure participant must abide by the following:

- Issuers that do not support an ACS for Visa Secure using EMV 3DS are automatically enrolled in the Visa Secure Attempts Server (where Visa will respond to authentication requests on behalf of the issuer with an attempt response that contains a CAVV) and the issuer is liable for any fraudulent transactions associated with specific reason codes. See Global Attempts Processing, Section 2.7.1, for details.
- **Effective 13 May 2024** Issuers are required to support a high protocol of EMV 3DS 2.2.0 for authentication transaction processing.

2.3 Acquirer Rules and Requirements

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

- Service Availability—Acquirers must notify their e-commerce merchants of the availability of Visa Secure and provide the service to their e-commerce merchants, as requested.
- Merchant Agreements—Merchant Agreements must be modified to reflect a merchant's participation in Visa Secure.
- Visa Secure Digital Certificates—Acquirers must assist 3DS Server Operators in obtaining digital certificates to support mutual authentication between the 3DS Server and the Visa Secure Directory Server.
- Security Requirements— Merchants and third-party commerce server providers must meet the security requirements for 3-D Secure processing, including support for the Payment Card Industry Data Security Standard (PCI DSS) for protecting card and cardholder information.
- Acquirer Approval—Contracts with third-party server providers or payment gateways must ensure that each merchant activated for Visa Secure is reported to and approved by the acquirer.

[13] See *EMV 3-D Secure Protocol and Core Functions Specification,* and *EMV 3-D Secure SDK Specification,* for details.

- Third Party Agent Registration—An acquirer who has contracted with a third-party service provider to provide Visa Secure services to its merchants must register third party
- 3DS Protocol Versions – Acquirers must ensure that their merchants send cardholder authentication transactions on the highest-protocol version supported by the issuer.

2.4 Card Type Restrictions (Non-Reloadable Visa Prepaid Cards)

Non-reloadable Visa prepaid cards are not required to participate in Visa Secure program. Although not required to participate, issuers may choose to include this card type in Visa Secure program by setting up the ISO BIN to participate in the service.

In terms of liability:

- Authentication—If a non-reloadable Visa prepaid card is authenticated during Visa Secure program (ECI 05), the merchant is protected against specific dispute reason codes.
- Attempted Authentication—If authentication is attempted on a non-reloadable Visa prepaid card (ECI 06), the merchant does not receive liability protection on e-commerce fraud-related disputes.

See *Visa Secure Program Dispute Resolution Guide* for more information on merchant dispute protection.

2.5 Dispute Protection and Exceptions

With Visa Secure program, merchants/acquirers are protected against e-commerce fraud-related disputes when the ECI is 05 or 06 and a CAVV is present in the authorization message.

2.5.1 Exceptions

There are exceptions to merchant dispute protection for ECI 05 and ECI 06 transactions. For these exceptions, the issuer can dispute:

Table 2–1: Merchant Dispute Protection Exceptions

Scope	Restriction	ECI	Description
Global	**CAVV Not Present**	ECI 05 or 06	VIP will downgrade the ECI 05 or 06 value to an ECI 07 when a CAVV is not present for PAN-based transactions. The downgrade can happen for domestic, international, and interregional transactions.

Scope	Restriction	ECI	Description
Global	**Non-Reloadable Prepaid**	ECI 06	Merchants are not protected when card type is a non-reloadable Visa prepaid card.
Global	**Visa Fraud Monitoring Program**	ECI 05 or 06	Merchants are not protected if they have been identified in the program. Merchant/acquirers in the program should submit Visa Secure transactions using ECI 07 and no CAVV.
U.S.	**Visa 3-D Secure Fraud Monitoring Program**	ECI 05 or 06	Merchants are not protected if they have been identified in the program. Merchants/acquirers in these programs should submit Visa Secure transactions using ECI 07 and no CAVV.
U.S.	**Custom Payment System (CPS) Requirements**	ECI 05 or 06	Merchants are not protected if transaction does not meet CPS requirements.
U.S.	**Merchant Restricted Merchant Category Codes (MCCs)**	ECI 05 or 06	Merchants are not protected if they are in one of the following MCCs: • MCC 4829—Money Transfer • MCC 5967—Adult Content and Services • MCC 6051—Non-Financial Institution-Foreign Currency, Non-Fiat Currency (for example: Cryptocurrency), Money Orders (Not Money Transfer), Account Funding (not Stored Value Load), Travelers Cheques, and Debt Repayment • MCC 7995—Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting and Wagers at Race Tracks • MCC 6540 - Non-Financial Institutions: Stored Value Card Purchase / Load • MCC 7801 - Government Licensed On-Line Casinos (On-Line Gambling) • MCC 7802 - Government-Licensed Horse/Dog Racing

2.6 CAVV Mandate

Participating issuers are required to provide a CAVV on authenticated (ECI 05) and approved Visa Data Only (ECI 07) transactions.

Merchants will receive a CAVV for authenticated and attempted authentication transactions which they must provide in the authorization message. For ECI 05 or ECI 06 transactions where a CAVV was not received in authorization, VisaNet will reclassify the ECI value to ECI 07. ECI 07 transactions are not protected from disputes.

2.7 Global Attempts Processing

When an issuer or their cardholder's account does not participate in Visa Secure or participates but their ACS is unavailable, the Visa Secure Attempts Server responds on their behalf. The response indicates that the merchant attempted to obtain authentication and provides the merchant with a CAVV. Where the Visa Secure Attempts Service responds on the issuer's behalf, the issuer will be liable for any e-commerce fraud-related disputes.

Visa assesses a fee to the issuer for providing a CAVV on its behalf as specified in the applicable Fee Guide.

2.7.1 Global Attempts Processing for EMV 3DS

If an issuer or their cardholder's account does not support Visa Secure with EMV 3DS or participates but their ACS is unavailable, Visa will respond to an authentication request on behalf of the issuer. Visa responds with a standard attempts response that contains a CAVV. Visa assesses a fee to issuers for providing a CAVV on its behalf as specified in the applicable Fee Guide.

Effective[14] **18 October 2024**, Visa Secure Attempts Server will use Smart Attempts service and respond on behalf of activated issuers for qualifying attempts transactions with a successful authentication response and Visa-generated CAVV. This applies to all activated issuers in AP (except India, Bangladesh, Nepal, Bhutan), Canada, CEMEA (except Albania, Azerbajan, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, and Ukraine), and LAC regions. Additionally, for the U.S. region, Visa Secure Smart Attempts only applies to activated, non-participating Visa Secure issuers in the U.S. who do not have an ACS defined. Visa Secure Attempts Server will respond with an (Authentication Attempted ECI 06) for issuers not activated for this processing or transactions that do not qualify for the service.

[14] Announced in Visa Business News AI14072 and AI140651.

2.7.2 Attempts Processing Exclusions

The Visa Secure Attempts Server will only stand in for transactions that are within scope of attempts processing. The following transaction types are excluded from the global attempts processing:

- The following 3DS Challenge Indicators:
    - (threeDSRequestorChallengeInd) = 05 No challenge requested (transactional risk analysis is already performed)
    - (threeDSRequestorChallengeInd) = 82 No challenge requested (utilize Secure Corporate Exemption as applicable)
- 3RI transactions (deviceChannel = 03) generally are excluded from global attempts processing.
    - Merchant-Initiated Transactions (MITs), identified by 3RI Indicator = 01 (Recurring Transaction), 02 (Installment Transaction), and 81 (Unscheduled Card-on-File) are within scope of attempts processing.
- NPA transactions (messageCategory = 02)
- Non-reloadable prepaid cards

2.8 Use of Authentication Data in Authorization

This section outlines the rules and requirements associated with the use of authentication data in different transaction types such as split shipments, delayed deliveries, recurring transactions, installment transactions, and online auctions.

2.8.1 Split Shipment and Delayed Delivery

The following outlines information on the use of authentication data in split shipments and delayed delivery:

- 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, only the second Authorization Request may be submitted with the original authentication data for the purchase. Any Authorization Request beyond the second must not include the original authentication data.
- 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 Visa Secure dispute protection and may be charged back by the issuer.

2.8.2 Time Limit and Amount Variation

Authentication data for a transaction must not be submitted in the authorization request for another transaction and merchants must adhere to the following limits associated with authentication data:

- 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.
- 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. Any authorization amount that exceeds 15% of the authenticated amount is not subject to Visa Secure dispute protection and may be charged back by the issuer.

2.8.3 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.

- First Authentication Transaction—Issuer should be aware that for merchants to receive dispute 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 Visa Secure transaction.
- Subsequent Authorization Transactions—All subsequent authorization requests in the recurring series must be processed as Recurring Transactions, using the Recurring Indicator.

  Recurring indicators vary based on acquirer region:

  - Recurring: US acquired: ECI = "02"
  - Non-US acquired: POS Environment Code = "R"
  - The merchant must follow guidance regarding CAVV storage and re-use as outlined in section 1.3.2.1 of this document.

- Because the first transaction was conducted via the Internet as a Visa Secure authenticated or attempted authentication, dispute protection applies to the original e-commerce transaction.
- For the subsequent Recurring Transactions, dispute provisions applicable to Recurring Transactions apply, and Visa Secure dispute protection may apply if the recurring transaction was authenticated via the 3RI device channel.
- Please refer to section 2.12.4 of this document and the Visa Secure – 3DS Requestor Initiated (3RI) User Guide and Best Practices for details on authentication of recurring / merchant-initiated transactions.

2.8.4 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.

An installment transaction is for a single good or service rather than an ongoing (or recurring) purchase. The transactions must have a specified end date.

- First Authentication Transaction
  - 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 first installment transaction received dispute protection from fraud related disputes for fully authenticated and attempted authentications.
- Subsequent Authorization Transactions—The remaining transactions are processed as installment transactions, so must not contain authentication data, specifically the ECI and the CAVV. Dispute liability protection for the acquirer/merchant does not apply to the subsequent installment transactions.
- Authentication Fields—The 'Instalment Payment Data' field in the Authentication Request message (AReq) is required when the merchant and cardholder have agreed to an installment payment option.

2.8.5 Online Auctions

Issuers should be aware that merchants offering 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 Authentication Request (AReq) to the authorization request.

Merchants must not re-use the CAVV for another transaction with the same cardholder (for example, on another auction).

2.9 ECI 06 Quality of Service Program

To help ensure a positive e-commerce experience for cardholders and protect the overall integrity of the Visa Secure, issuers are not permitted to establish authorization processing criteria where transactions submitted as attempted authentications (ECI 6) are blanket declined. Standards and penalties have been defined in the Visa Rules.

See *Appendix B.2: ECI 06 Quality of Service Program* for more details.

2.10 Authorization Processing

For a Visa Secure transaction, an acquirer/merchant must submit the same ECI value in clearing that was submitted in authorization. Applies to ECI 05 and ECI 06. **Effective through 14 April 2024** If the ECI values are not the same, the acquirer/merchant will not receive fraud liability protection. **Effective 15 April 2024** all fraud dispute rights for Visa Secure will be determined based on authorization data only.

2.11 Authentication Approval Rates (U.S. Only)

U.S. issuers must operate their Visa Secure program such that 95% of authentication transactions are approved responses, excluding attempted authentication transactions.

2.12 EMV 3DS Requirements

2.12.1 Minimum Data Requirements for EMV 3DS

Merchants must provide the data elements in Visa Secure authentication message as follows: 1) required always and 2) required if available. Merchants are also required to use the 3DS Method if the Method URL is provided. Providing Visa Secure data is subject to regional and country regulations.

2.12.2 Visa Secure Performance Program with EMV 3DS

To help ensure a positive e-commerce experience for cardholders, provide enhanced risk-based decision making, and protect the overall integrity of Visa Secure, issuers who are processing EMV 3DS transactions must comply with the following performance requirement for EMV 3DS transactions.

2.12.2.1 Risk-based Authentication (RBA)

Issuers are required to support RBA for EMV 3DS. Issuers must evaluate the risk level of each transaction using some form of risk-model, rules engine, or risk analysis. Issuers must apply the following authentication procedure:

- Low risk transactions – no step-up (frictionless authentication)[15]

Issuers may also apply one or both of the following authentication procedures:

- Higher risk transactions – step-up may be performed (recommend no more than 5%)
- Very high-risk transactions – may decline with no further cardholder interaction

2.12.2.2 Authentication Response Time Threshold

An issuer must respond to the original authentication request (i.e., AReq) within 5 seconds. If an issuer does not respond within the time threshold, Visa will provide an attempts response on behalf of the issuer. The issuer will be liable for fraud related disputes on these transactions.

See EMV 3-D Secure Protocol and Core Functions Specification, Section 5.5 for more details.

2.12.2.3 Abandonment Rate Threshold

Cardholder authentication abandonment rate on EMV 3DS transactions must not exceed 5%. Abandonment rate is calculated monthly as follows: (count of transactions a cardholder abandons[16] or selects "cancel") divided by the total number of authentication requests.

Issuers that do not comply with the rule must provide a performance improvement plan. If no improvements are made after four months from first identification in the program, non-compliance assessments may be applied starting month five.

2.12.3 Issuer Access Control Server (ACS) Availability with EMV 3DS

For AP, CEMEA, LAC, and NA an issuer's ACS must be available 99% of the time. Availability will be measured by number AReq message timeouts / total number of AReq messages.

For EU, an issuers ACS must be available 99.9% of the time. Availability will be measured by number AReq message timeouts / total number of AReq messages.

[15] May not apply to regulated markets requiring strong authentication (e.g., cardholders providing additional information).
[16] Exclude ARes challenge requests the merchant opts-out of, and RReq responses where the merchant cancelled the CReq/CRes prior to the minimum Visa challenge time limit of 60 seconds

2.12.4 3DS Requestor Initiated (3RI) Transactions

- Refer to the Visa Secure – 3DS Requestor Initiated (3RI) User Guide and Best Practices for details.
- Effective April 15, 2025, Visa Secure supports authentication of standing-instruction merchant-initiated transactions, including recurring, installment and unscheduled card-on-file transactions. Only issuing BINs in AP, Canada, CEMEA, EU, and LAC are enabled as of this effective date.

2.12.5 Non-Payment (NPA)

- If a merchant sends an NPA Authentication Request (AReq) for 3DS Requestor Authentication Indicator "04 = Add Card or 05 = Maintain Card" the following will apply:
  - If the transaction was successfully authenticated with a challenge, the Results Request (RReq) must contain an ECI 05 and a CAVV.
  - Effective through 15 October 2022, If the transaction is authenticated without a challenge (i.e., frictionless), the ECI and CAVV are not required.
  - Effective 16 October 2022, If the transaction is successfully authenticated without a challenge (i.e., frictionless, the Authentication Response (ARes) must contain ECI 05 and CAVV
  - If a 3DS Server sends a NPA AReq with 3DS Requestor Authentication Indicator of "06 = Cardholder Verification as part of EMV token ID&V" an issuer must respond with a challenge request and the 3DS Server must proceed with initiating the challenge.
  - If a merchant sends an NPA as part of a 3DS Requestor Initiated (3RI) authentication request (e.g., a merchant-initiated authentication request when the cardholder is not available) and the transaction is successfully authenticated, the ECI and CAVV are not required. 3RI NPA Values are:
    - 03 – Add Card
    - 04 – Maintain Card
    - 05 – Account Verification
- All issuers must support and respond to NPA transactions.

2.12.6 Authentication on Behalf

Authentication on Behalf is defined as a merchant or entity performing the authentication but does not submit the subsequent authorization.

Effective 23 April 2022, if a merchant or entity is performing authentication on behalf, they must follow the following requirements:

- Entity/Merchant must register as Merchant Servicer with Visa in the Third-Party Agent

Program

- Entity/Merchant must use the following criteria in authentication and authorization for authentication on behalf of one merchant:
  - The name of the merchant performing authentication and the merchant of record must be included in the authentication message with cardholder present
    - The required format is "merchant authenticating* merchant of record". The merchant of record must match the name submitted in VisaNet (BASE I/SMS and BASE II) transactions.
  - Acquiring BIN/Merchant ID can differ between authentication and authorization
- Entity/Merchant must use the following criteria in authentication and authorization for authentication on behalf of multiple merchant:
  - Merchant/Entity performing authentication submits the merchant/entity name and full amount of purchase with the cardholder present
- A unique CAVV must be obtained for each merchant
- Merchant/Entity must submit a unique 3RI request for each merchant of record following using the following format:
  - The required format is "merchant authenticating* merchant of record" The merchant of record must match the name submitted in VisaNet (BASE I/SMS and BASE II) transactions.

2.12.7 Routing of Authentication Requests Through a Non-Visa Directory Server

Effective 23 April 2022, Issuers and acquirers that route authentication request to a non-Visa Directory Server (DS), must adhere to the following requirements:

- Issuers and acquirers must register the non-Visa Directory Server (DS) provider as a third-party agent and confirm the DS provider has completed the 3DS Security program
- If non-Visa Directory Server is unavailable, Visa transactions must be routed to the Visa DS.
- International authentication requests processed through the Visa DS
- All EMV 3DS transactions must comply with EMVCo specifications.
- Ensure the non-Visa DS does all of the following:
  - Uses EMVCo approved software, including the latest version of the specification that is available (within 6 months of EMVCo Testing Availability) and is valid
  - Adheres to system availability performance standards (99.999%)
  - Supports attempts processing capabilities
  - Supports Visa defined values and functionality
  - Has a 5 second timeout when waiting for the ARes response. If no response the domestic DS must provide an attempts response
- Supports Visa required data elements (enforcing these data elements are sent)

- Supports Visa extensions (e.g., acquirer country code)
- Supports Visa SCA programs/solutions
- Supports Visa's CAVV or equivalent cryptogram
- Supports Visa's ECI values or equivalent
- Parties operating a non-Visa DS will also be subject to the additional monthly reporting requirements below. Contact your Visa representative for further information.
  - The total number of authentication requests/responses
  - Data from the following Performance Programs:
    - Cardholder abandonment rate
    - ACS latency
    - ACS availability
    - Authentication step-up rate

2.12.8 Europe & Payment Services Directive 2 (PSD2)

To take advance of the exemptions Visa's recommends supporting EMV 3DS v2.2. Please reference the following materials available on Visa Access to assist with planning and implementing SCA compliance polices and solutions:

- Preparing for PSD2 SCA
- PSD2 SCA for Remote Electronic Transactions: Implementation Guide
- Addendum: Implementing SCA for Travel & Hospitality
- Trusted Listing Implementation Guide
- Delegated Authentication Implementation Guide

2.12.9 Visa Secure Issuer Authentication Challenge Rate Requirement – AP Region

Effective 23 April 2022 for AP except Bangladesh, China, India, Japan, Mongolia, Nepal, Republic of Korea, Taiwan

Effective 15 April 2023 for Japan

An issuer must not exceed the challenge rate for EMV 3DS transaction as specified in Table 2-2: Issuer Challenge Rate on EMV 3DS transaction – AP Region

Table 2–2: Merchant Dispute Protection Exceptions

Country	Challenge Rate Threshold[17]
Cambodia, Guam, Hong Kong, Laos, Macao, Myanmar, Philippines, Singapore, Thailand, Vietnam	75%
American Samoa, Australia (including Cocos [Keeling] Islands, Heard Island and McDonald Islands, Norfolk Island, Lord Howe Island, Macquarie Island), Cook Islands, Fiji (including Rotuma Island), French Polynesia, Japan[18], Kiribati (including Canton and Enderbury Islands, Christmas Island (Kiritimati), Fanning Island, Malden Island, Starbuck Island, Washington Island), Marshall Islands, Micronesia, Nauru, New Caledonia, New Zealand (including Antipodes Island, Auckland Island, Bounty Island, Campbell Island, Chatham Island, Kermadec Island, Stewart Island), Northern Mariana Islands, Niue, Papua New Guinea, Pitcairn Islands, Samoa, Solomon Islands, Timor-Leste, Tokelau, Tonga, Tuvalu, US Minor Outlying Islands (including Baker Island, Howland Island, Jarvis Island, Johnston Island, Midway Island, Palmyra Island, Wake Island), Vanuatu, Wallis and Futuna	50%
Bhutan, British Indian Ocean Territory, Brunei, Crozet Islands, Indonesia, Kerguelen Island, Malaysia, Maldives, Mascarene Islands, Palau, Pescadores Island, Rodrigues Island, St. Paul Island, Sri Lanka	Not Applicable

2.13 Country Rules

Specific country rules exist for participation in Visa Secure.

See *Appendix B.1: Visa Country Rules and Local Regulatory Rules* for more details.

2.14 User Interface Requirements

Visa Secure badge, artwork, reproduction, and application guidelines can be accessed through Visa Access or at www.productbrandstandards.com

[17] The threshold is based on an individual market's risk-based authentication performance benchmarks.
[18] Effective 15 April 2023

2.14.1 Issuer User Interface Requirements

The ACS must comply with specific user interface requirements and only use the Visa master brand logo on frictionless and challenge screens.

See Visa Secure User Experience Guidelines available on Visa Developers Partner webpage for more details. https://developer.visa.com/pages/visa-3d-secure

Use of the Visa Secure badge is optional on checkout page and website. However, if branding for competing payment authentication programs are displayed, the Visa Secure badge must also be displayed.

Visa master brand and Visa Secure badge, artwork, reproduction, and application guidelines can be accessed through Visa Access or at www.productbrandstandards.com

2.14.2 Merchant User Interface Requirements

Use of the Visa Secure badge is optional on checkout page and website. However, if branding for competing payment authentication programs are displayed, the Visa Secure badge must also be displayed.

If the merchant displays the Visa Secure badge on its website, use of the mark must comply with the Visa Product Brand Standards.

Visa Secure badge, artwork, reproduction, and application guidelines can be accessed through Visa Access or at www.productbrandstandards.com

2.15 Authentication and Authorization Data

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

Table 2–3: Authorization & Authentication Fields

VisaNet Field Description	Comments
Acquirer Identifier (BIN)	This field must match the acquirer Identifier used in the Verify Enrollment Request or Authentication Request. This field also **must** match the acquirer identifier submitted in VisaNet (BASE I/SMS and BASE II) transactions.[19]
Merchant Identifier (ID) Number	This field must match the Merchant ID used in the Verify Enrollment Request or Authentication Request. This field also **must** match the Merchant ID used by the acquirer in VisaNet (BASE I/SMS and BASE II) transactions.[20]
Merchant Name	This field must contain the name of the 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. **Travel Agencies:** For transactions booked through travel agencies, the name of the travel merchant[20] as the merchant of record must be included in the authentication message. The required format is "travel agency name* travel merchant" The travel merchant name must match the name submitted in VisaNet (BASE I/SMS and BASE II) transactions.

[19] If a merchant uses multiple acquirers, a different acquirer may be used for authentication and VisaNet processing (i.e., BASE I/SMS and BASE II. When different acquirers are used, the acquirer identifier and Merchant ID submitted in the authentication message do not have to match those identifiers in the VisaNet transactions (i.e., BASE I/SMS and BASE II)
[20] Travel merchant is defined as a seller or provider of goods and services

2.16 Digital Authentication Framework using EMV 3DS

The Digital Authentication Framework (DAF) outlines an expanded set of capabilities and requirements to enable merchants to deliver frictionless shopping experiences while ensuring effective fraud management for eCommerce transactions. Under the framework, Visa is expanding the criteria for fully authenticated digital transactions and the associated fraud dispute rules. The Digital Authentication Framework outlines an approach for a consistent and verifiable set of transaction data that can increase issuer confidence and facilitate risk decisions that lead to increased approval rates and lower fraud. The program defines a unique type of payment credential referred to as an Authenticated Payment Credential. Merchants that meet the program criteria on qualified purchase transactions will receive fraud dispute protection.

EMV 3DS provides the mechanism for a merchant to provide the required data and enables an issuer to authenticate the cardholder account ID.

The rules will be **effective 15 April 2023 for merchants in Japan and 23 April 2022 for merchants in AP[21], CEMEA, Europe, LAC, Canada, and US regions**. Merchant participation in DAF is optional and subject to meeting the program requirements. Merchants will be required to register and will be assigned a Visa approved merchant identifier.

The rules will be **effective 15 April 2023 for issuers in Japan, 23 April 2022 for issuers in AP[21], CEMEA, Europe, and LAC regions, and 19 October 2024 for issuers in Canada.** Issuer participation is strongly encouraged. Issuer participation will be required **effective 12 April 2024 for issuers in Japan, 15 April 2023 for issuers in AP[21], CEMEA, Europe, and LAC regions, and 18 October 2025 for issuers in Canada.**

Effective 15 April 2023, Visa may provide a stand-in response on behalf of non-participating Issuers when a merchant submits an authentication request containing an Authenticated Payment Credential, and Issuers will retain the fraud liability.

Transaction processing requirements are outlined below. Additional program requirements and fraud dispute rules are outlined in the PSRs.

2.16.1 Transaction Requirements

Effective 15 April 2023 for Japan, **23 April 2022 for AP[21], CEMEA, Europe, and LAC regions, and 19 October 2024 for Canada,** issuers are prohibited from requesting a challenge in EMV 3DS on authentication requests from a merchant presenting an Authenticated Payment Credential that meet

[21] Excluding Bangladesh, India, and Nepal

the merchant requirements listed below. The issuer will only have the ability to decline an authentication request deemed high-risk by a Visa risk assessment[22]. Merchants must submit an authentication request with the DAF appropriate indicators, include a Visa approved merchant identifier (i.e., Visa Merchant ID - VMID) and the required data elements listed below in Appendix A: Visa Secure with EMV 3DS Minimum Data Requirements**.**

2.16.2 Authentication Performance Thresholds

Effective 15 April 2023 for Japan, 23 April 2022 for AP[15], CEMEA, Europe, and LAC regions, and 19 October 2024 for Canadian issuers, the Authentication Success Rate on DAF transactions processed through Visa Secure using EMV 3DS must be equal to or higher than 95%. The authentication success rate threshold only applies when an issuer has more than 500 DAF transactions for the month.

The Authentication Success Rate is measured monthly on DAF authentications by dividing the number of successful authentication responses by the total number of authentication requests minus responses when the merchant chooses to not proceed with a challenge request. "Issuer SCA Required" declines will also be removed for Europe domestic and intraregional authentications.

Authentication Success Rate	=	(SUM (ARes with Transaction Status "Y") + SUM (RReq with Transaction Status 'Y')) / (SUM (All AReqs sent to the issuer's ACS) - SUM (Requests (RReq) with a Transaction Status = "N" with a Transaction Status Reason = 14 (Transaction timed out at the ACS) and a Challenge Cancel Indicator = 05 (First CReq not received)) - (SUM (ARes with Transaction Status "N" with a Transaction Status Reason = "Issuer SCA Required") for Europe domestic and intraregional authentications)

2.16.3 Authorization Performance Thresholds

Effective 15 April 2023 for Japan, 23 April 2022 for AP[15], CEMEA, Europe, and LAC regions, and 19 October 2024 for Canadian issuers, the Authorization Approval Rate on DAF authorizations must be 95% or higher for domestic and 90% or higher for international[23] authorizations. Also, the total DAF authorizations must exceed 500 transactions for the authorization performance threshold to be

[22] For Europe domestic and intraregional Transactions, European issuers may also decline low risk domestic and intraregional authentication requests that are not authenticated under the Visa Delegated Authentication Program or other arrangements in force with issuers for SCA delegation. The only permitted decline reason in those cases is "Issuer SCA Required".
[23] International transactions for Europe include intraregional and interregional transactions

applicable. The Authorization Approval Rate is measured monthly on DAF authorizations as shown below[24]:

Domestic Authorization = Approval Rate	***"Approved" + "No Reason to Decline" domestic Authorization Responses for AP, CEMEA, LAC, and EU***
	All domestic Authorization Responses for AP, CEMEA, EU, LAC – SCA Declines with FIDO data (in accordance with Visa's FIDO requirements) for Europe domestic DAF transactions using EMV 3DS – SCA Declines for Europe domestic DAF transactions using Visa Token Service (VTS)
International Authorization = Approval Rate	"Approved" + "No Reason to Decline" international Authorization Responses for AP, CEMEA, LAC, and EU intraregional and interregional transactions
	All international Authorization Responses for AP, CEMEA, EU, LAC – SCA Declines with FIDO data (in accordance with Visa's FIDO requirements) for Europe intraregional DAF transactions using EMV 3DS - SCA Declines for Europe intraregional DAF transactions using Visa Token Service

2.17 Visa Secure On-Behalf-Of-Issuer Services

Visa Secure On-Behalf-Of-Issuer Services is an opt-in service that offers secure authentication for Visa B2B Virtual Card accounts and Visa pseudo accounts. Because these accounts are linked to organizations rather than individuals, step-up (challenge) authentication is not possible. With this enhancement, Visa Secure Directory Server (DS) will allow a default for both Virtual and Pseudo Account traffic to fully authenticated without step-up authentication. This default applies to Issuer BIN or account ranges for Issuers who have opted-in to the service. These transactions will not be forwarded to the Issuer's ACS.

Visa B2B Virtual Account: Visa B2B Virtual Payment cards, or Virtual Accounts, are non-plastic one-time or multi use credentials used within commercial card payment flows. Examples include lodged virtual accounts, where the same card number is used for the same supplier and limited use cards enabling online travel agencies, travel service providers, and other travel payment providers to pay travel suppliers for inventory. These accounts are not set up with Visa Payables Automation, but rather

[24] Excludes Prepaid Cards

in-house by the issuer or through a 3rd party. Issuers looking to enroll Visa B2B Virtual Accounts for the first time should contact their regional client support.

Visa Pseudo Account: A Visa pseudo account is a type of Visa virtual card account, which originates from the Visa Token Service (VTS) created in Visa Payables Automation (VPA). Visa Pseudo Accounts power many of the products in Visa Business Solutions (VBS) and support numerous use cases including travel, payables, and purchasing. Issuers looking to enroll pseudo accounts with Visa Payables Automation for the first time should contact their regional client support.

2.18 Visa Data Only Program

The Visa Data Only (VDO) Program uses the existing EMV 3DS information only infrastructure to provide merchants a risk and authentication program construct that supports an uplift in authorization approval rates while helping to mitigate fraud without any added friction to the e-commerce checkout flow.

A merchant that chooses to use Visa Data Only will send the cardholder's issuer an AReq with a "Data Only" flag. The issuer's ACS reviews this enhanced data from the merchant, and if approved, returns a transaction status "I", ECI 07 and CAVV to the Visa Secure Directory Server. Under the VSDO Program, merchants do not receive fraud liability protection on Data Only transactions. Issuers cannot force a cardholder account ID authentication challenge for Data Only transactions.

Visa Data Only Program Requirements

VDO Program participants must:

- Complete Visa's EMV 3DS 2.2 program enrollment process
- Ensure that the participant's Visa Secure EMV 3DS 2.2 program component has successfully met EMV 3DS 2.2 Compliance Testing Program requirements and Visa Secure EMV 3DS 2.2 product testing.
- Only use a digital certificate issued by or associated with Visa as an authentication mechanism for a Visa product or service.
- Adhere to the EMV 3DS 2.2 data inclusion requirements.
- Ensure that a CAVV version 7 is used

2.18.1 Issuer Requirements for Visa Data Only

Effective **1 September 2019**, all issuers participating in the Visa Secure program must support and respond to all Visa Data Only (information-only authentication requests for EMV 3DS) in authentication for EMV 3DS 2.2 transactions.

Effective through 11 April 2025, Issuers must respond with either an approved authentication response and an ECI 07 and a CAVV, or a failed authentication response.

Effective 12 April 2025, Issuers must respond with an approved authentication response including an ECI 07, CAVV, and transaction status 'I'. Issuers can no longer respond with a failed authentication response. If Issuers fail to respond correctly, the Visa Secure Directory Server will provide a stand-in response.

A Visa Secure with EMV 3DS Minimum Data Requirements

Merchants must provide the data elements in EMV 3DS authentication message (AReq) as follows: 1) required always and 2) required conditional. Merchants are also required to use the 3DS Method if the Method URL is provided by the issuer. Providing EMV 3DS data is subject to regional and country regulations. The merchant data has been categorized into seven groups.

Effective 12 August 2024, Merchants in AP, EU, LAC, and NA must submit the following data elements in their EMV 3DS AReq for data quality monitoring:

Browser Transactions	App/SDK Transactions
• Browser IP Address • Cardholder Email Address OR Cardholder Phone Number *(At least 1 of these fields must be provided from work, home, or mobile)* • Cardholder Name	• Common Device Identification Parameters (Device IP Address) • Cardholder Email Address OR Cardholder Phone Number *(At least 1 of these fields must be provided from work, home, or mobile)* • Cardholder Name

Effective 12 August 2024, Merchants in CEMEA must submit the following data elements in their EMV 3DS AReq for data quality monitoring:

Browser Transactions	App/SDK Transactions
• Browser IP Address	• Common Device Identification Parameters (Device IP Address)
Data Element Categorization:Message Inclusion	**Device Channel**
R = Required C = Required Conditional[25] O = Optional	A = App B = Browser 3 = 3RI

A.1 Transactional and Checkout Page Information

Table A–4: Transactional and Checkout Page Information[26]

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Framework[27]	Device Channel
3DS Method Completion Indicator	R	R	R	B
3DS Requestor Authentication Indicator	R	R	R	A/B
3DS Requestor Authentication Information	O	O	O	A/B
3DS Requestor Challenge Indicator	O	O	O	A/B
3DS Requestor Decoupled Requestor Max Time	O	O	O	A/B/3
3DS Requestor Decoupled Requestor Indicator	O	O	O	A/B/3
3DS Requestor ID	R	R	R	A/B/3
3DS Requestor Name	R	R	R	A/B/3

[25] Sender shall include the data element in the identified Message Type if the Conditional Inclusion requirements are met; Recipient shall check for data element presence and Validate data element contents. When no data is to be sent data element, the data element should be absent. See EMV 3DS Specifications for Conditional Inclusions
[26] Based on EMV 3DS 2.2.0 specification.
[27] Regional/country level adjustments may be applied to address specific market conditions.

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Framework[27]	Device Channel
3DS Requestor Prior Transaction Authentication Information[28]	C	C	C	A/B/3
3DS Requestor URL	R	R	R	A/B/3
3DS Server Reference Number	R	R	R	A/B/3
3DS Server Operator ID[29]	R	R	R	A/B/3
3DS Server Transaction ID	R	R	R	A/B/3
3DS Server ULR	R	R	R	A/B/3
3RI Indicator[30]	R	R	R	3
Account Type	C	C	C	A/B/3
Acquirer BIN	R	R	R	A/B/3
Acquirer Merchant ID	R	O	R	A/B/3
Address Match Indicator	O	O	O	A/B
Broadcast Information	C	C	C	A/B/3
Browser Accept Headers	R	R	R	B
Browser IP Address	R	C	R	B
Browser Java Enabled	C	C	C	B
Browser JavaScript Enabled	R	R	R	B
Browser Language	R	R	R	B
Browser Screen Color Depth	C	C	C	B
Browser Screen Height	C	C	C	B
Browser Screen Width	C	C	C	B
Browser Time Zone	C	C	C	B

[28] Condition is for a 3RI transaction and Message Category is Payment (01)
[29] Visa required data element. Must be present or Visa DS will reject the transaction.
[30] Required for Device Channel -03 – 3RI

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Framework[27]	Device Channel
Browser User-Agent	R	R	R	B
Card/Token Expiry Date[29]	R	O	R	A/B/3
Cardholder Account Information	O	O	O	A/B/3
Cardholder Account Number	R	R	R	A/B/3
Cardholder Account Identifier	O	O	O	A/B/3
Cardholder Billing Address City	C	C	R[31]	A/B/3
Cardholder Billing Address Country	C	C	R[29]	A/B/3
Cardholder Billing Address Line 1	C	C	R[29]	A/B/3
Cardholder Billing Address Line 2	C	C	C	A/B/3
Cardholder Billing Address Line 3	C	C	C	A/B/3
Cardholder Billing Address Postal Code	C	C	R[29]	A/B/3
Cardholder Billing Address State	C	C	R[29]	A/B/3
Cardholder Email Address	R[32]	C	R[29]	A/B/3
Cardholder Home Phone Number	R[31]	C	C	A/B/3
Cardholder Mobile Phone Number	R[32]	C	R	A/B/3
Cardholder Name	R	C	C	A/B/3
Cardholder Shipping Address City	C	C	C	A/B/3
Cardholder Address Country	C	C	C	A/B/3
Cardholder Shipping Address Line 1	C	C	C	A/B/3
Cardholder Shipping Address Line 2	C	C	C	A/B/3
Cardholder Shipping Address Line 3	C	C	C	A/B/3
Cardholder Shipping Address Postal Code	C	C	C	A/B/3

[31] Only one data field is required between cardholder name OR cardholder phone number; only 1 phone number is required out of home, mobile, or work

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Framework[27]	Device Channel
Cardholder Shipping Address State	C	C	C	A/B/3
Cardholder Work Phone Number	R[31]	C	C	A/B/3
Device Channel	R	R	R	A/B/3
Device Information	R	C	C	A
Device Rendering Options Supported	R	R	R	A
EMV Payment Token Indicator	C	C	C	A/B/3
EMV Payment Token Source	C	C	C	A/B/3
Installment Payment Data	C	C	C	A/B/3
Merchant Category Code	R	O	R	A/B/3
Merchant Country Code	R	O	R	A/B/3
Merchant Name	R	O	R	A/B/3
Merchant Risk Indicator	O	O	O	A/B/3
Message Category	R	R	R	A/B/3
Message Extension	C	C	C	A/B/3
Message Type	R	R	R	A/B/3
Message Version Number	R	R	R	A/B/3
Notification URL	R	R	R	B
Purchase Amount	R	C	R	A/B/3
Purchase Currency	R	C	R	A/B/3
Purchase Currency Exponent	R	C	R	A/B/3
Purchase Date & Time	R	C	R	A/B/3
Recurring Expiry	C	C	C	A/B/3
Recurring Frequency	C	C	C	A/B/3
SDK App ID	R	R	R	A
SDK Encrypted Data	C	C	C	A
SDK Ephemeral Public Key (Qc)	R	R	R	A

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Framework[27]	Device Channel
SDK Maximum Timeout	R	R	R	A
SDK Reference Number	R	R	R	A
SDK Transaction ID	R	R	R	A
Transaction Type[29]	R	N/A	R	A/B/3
Whitelist Status	C	C	C	A
Whitelist Status Source	O	O	O	A/B/3

A.2 3DS Requestor Authentication Information

Table A–5: 3DS Requestor Authentication Information

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Program	Device Channel
3DS Requestor Authentication Method	O	O	O	A/B
3DS Requestor Authentication Timestamp	O	O	O	A/B
3DS Requestor Authentication Data	O	O	O	A/B

A.3 3DS Requestor Prior Transaction Authentication Information

Table A–6: 3DS Requestor Prior Transaction Authentication Information

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Program	Device Channel
3DS Requestor Prior Transaction Reference[32]	C	C	C	A/B/3
3DS Requestor Prior Transaction Authentication Method	O	O	O	A/B/3

[32] Condition is a 3DS Requestor Initiated Transactions (3RI) and Message Category is Payment (01)

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Program	Device Channel
3DS Requestor Prior Transaction Authentication Timestamp	O	O	O	A/B/3
3DS Requestor Prior Transaction Authentication Data	O	O	O	A/B/3

A.4 Merchant Risk Indicator

Table A–7: Merchant Risk Indicator

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Program	Device Channel
Shipping Indicator	O	O	O	A/B/3
Delivery Timeframe	O	O	O	A/B/3
Delivery Email Address	O	O	O	A/B/3
Reorder Items Indicator	O	O	O	A/B/3
Pre-Order Purchase Indicator	O	O	O	A/B/3
Pre-Order Date	O	O	O	A/B/3
Gift Card Amount	O	O	O	A/B/3
Gift Card Currency	O	O	O	A/B/3
Gift Card Count	O	O	O	A/B/3

A.5 Cardholder Account Information

Table A–8: Cardholder Account Information

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Framework	Device Channel
Cardholder Account Age Indicator	O	O	O	A/B/3
Cardholder Account Date	O	O	O	A/B/3
Cardholder Account Change Indicator	O	O	O	A/B/3

Data Element	Message Category - Payment	Message Category - Non-Payment	Digital Authentication Framework	Device Channel
Cardholder Account Change	O	O	O	A/B/3
Cardholder Account Password Change Indicator	O	O	O	A/B/3
Cardholder Account Password Change	O	O	O	A/B/3
Shipping Address Usage Indicator	O	O	O	A/B/3
Number of Transactions Day	O	O	O	A/B/3
Number of Transactions Year	O	O	O	A/B/3
Number of Provisioning Attempts Day	O	O	O	A/B/3
Cardholder Account Purchase Count	O	O	O	A/B/3
Suspicious Account Activity	O	O	O	A/B/3
Shipping Name Indicator	O	O	O	A/B/3
Payment Account Age Indicator	O	O	O	A/B/3
Payment Account Age	O	O	O	A/B/3

A.6 Device Information

Device Information must adhere to the Visa Device ID requirements.

Additionally, the Common Device Identification Parameters Available in All Platforms – C010 - IP Address must be included for DAF transactions.

A.7 3DS Method

The merchant checkout page must load the ACS 3DS Method URL, if the 3DS Method URL is present, which allows the ACS to obtain additional browser information for risk-based decision making.

A.8 Digital Authentication Framework (DAF) Extension

Merchants must include the DAF Extension in the Authentication Request (AReq).

Merchants must include the Cardholder Account Requestor ID in the DAF extension for DAF transactions.

B Visa Country Rules and Visa Programs

- Visa Country Rules and Local Regulatory Rules
- Attempted Authentication Quality of Service Program
- Visa Secure Global Performance Enhancement Program

B.1 Visa Country Rules and Local Regulatory Rules

Acquirers and issuers must comply with specific country rules and, where applicable, regulatory rules. This section outlines the rules which are organized by country within each Visa region.

For more information, see *Visa Core Rules and Visa Product and Service Rules*.

Table B–1: Visa Country/ Region /Territory Rules and Local Regulatory Rules

Country/ Region/Territory	Visa Rule or Regulatory Rule	Rule
All Regions		
All Regions	**Visa Issuers**	When an issuer or their cardholder's account does not participate in Visa Secure or participates but their ACS is unavailable, the Visa Secure Attempts Server responds on their behalf. The response indicates that the merchant attempted to obtain authentication and provides the merchant with a CAVV. Visa assesses a fee to the issuer for providing a CAVV on its behalf as specified in the applicable Fee Guide.
Asia Pacific		
Australia	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33] for: • Visa credit[34], Visa debit[34], Reloadable Prepaid Cards

[33] Effective **15 October 2022** in Visa Secure with EMV 3DS
[34] This does not apply to Virtual Accounts associated with Visa Commercial Cards

	Visa Acquirers	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction uses Visa Secure using EMV 3DS if it is assigned any of the following MCCs: • 4722 (Travel Agencies and Tour Operators) • 4816 (Computer Network/Information Services) • 4829 (Wire Transfer Money Orders) • 5085 (Industrial Supplies) • 5311 (Department Stores) • 5399 (Miscellaneous General Merchandise) • 5411 (Grocery Stores and Supermarkets) • 5661 (Shoe Stores) • 5691 (Men's and Women's Clothing Stores) • 5699 (Miscellaneous Apparel and Accessory Shops) • 5722 (Household Appliance Stores) • 5732 (Electronics Stores) • 5733 (Music Stores – Musical Instruments, Pianos, and Sheet Music) • 5734 (Computer Software Stores) • 5912 (Drug Stores and Pharmacies) • 5943 (Stationery Stores, Office and School Supply Stores) • 5944 (Jewelry Stores, Watches, Clocks, and Silverware Stores) • 5999 (Miscellaneous and Specialty Retail Stores) • 6211 (Security Brokers/Dealers) • 7011 (Lodging – Hotels, Motels, Resorts, Central Reservation Services) • 7832 (Motion Picture Theaters) • 7995 (Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks) • 8999 (Professional Services) • 9402 (Postal Services – Government Only) Effective 15 October 2022 Ensure that its Electronic Commerce Merchant is enabled to process an Electronic Commerce Transaction using Visa Secure with EMV 3DS. If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Cambodia	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33] for: • Visa credit, Visa debit

	Visa Acquirers	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following MCCs: • MCC 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls through Use of Magnetic Stripe Reading Telephones, and Fax Services) • MCC 8398 (Charitable Social Service Organizations) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Hong Kong	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33]: for • Credit Cards • Debit Cards
	Visa Acquirer	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following MCCs: • MCC 4722 (Travel Agencies and Tour Operators) • MCC 4812 (Telecommunication Equipment and Telephone Sales) • MCC 5045 (Computers and Computer Peripheral Equipment and Software) • MCC 5621 (Women's Ready-To-Wear Stores) • MCC 5691 (Men's and Women's Clothing Stores) • MCC 5732 (Electronics Stores) • MCC 5734 (Computer Software Stores) • MCC 5816 (Digital Goods – Games) • MCC 5945 (Hobby, Toy, and Game Shops) • MCC 5999 (Miscellaneous and Specialty Retail Stores) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
India	**Regulatory Rule, Reserve Bank of India (RBI)**	All e-commerce transactions (including Mail Order/Telephone Order and Interactive Voice Response) are required to support 2FA (Visa Secure)

	Visa Issuers	An Issuer must participate in Visa Secure, as follows: • Credit Cards , Debit Cards, Reloadable Prepaid Cards An Issuer must authorize only a domestic Electronic Commerce Transaction with an Electronic Commerce Indicator 5 (Secure Electronic Commerce Transaction).
	Visa Acquirers	Ensure that its Electronic Commerce Merchant processes Electronic Commerce Transactions using Visa Secure Not process a domestic Electronic Commerce Transaction unless the Cardholder account ID has been successfully authenticated using Visa Secure
Indonesia	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33] for: • Credit Cards • Debit Cards
	Visa Acquirers	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following: MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5999 (Miscellaneous and Specialty Retail Stores) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Japan	**Industry Rule, Japan Online Gaming Association (JOGA)**	All JOGA members are strongly requested to implement Visa Secure
Macau	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33] for: • Credit Cards • Debit Cards

	Visa Acquirer	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following MCCs: • MCC 4722 (Travel Agencies and Tour Operators) • MCC 4812 (Telecommunication Equipment and Telephone Sales) • MCC 5045 (Computers and Computer Peripheral Equipment and Software) • MCC 5621 (Women's Ready-To-Wear Stores) • MCC 5691 (Men's and Women's Clothing Stores) • MCC 5732 (Electronics Stores) • MCC 5734 (Computer Software Stores) • MCC 5816 (Digital Goods – Games) • MCC 5945 (Hobby, Toy, and Game Shops) • MCC 5999 (Miscellaneous and Specialty Retail Stores) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Malaysia	**Visa Issuers**	An Issuer must participate in both Visa Secure with 3-D Secure 1.0[33] and Visa Secure with EMV 3DS[33]: • Credit Cards • Debit Cards
	Visa Acquirers	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following: MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 5977 (Cosmetic Stores) • MCC 5999 (Miscellaneous and Specialty Retail Stores) • MCC 7011 (Lodging – Hotels, Motels, Resorts, Central Reservation Services) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
New Zealand	**Visa Issuers**	An Issuer must participate in both Visa Secure with 3-D Secure 1.0 and Visa Secure with EMV 3DS[33], as follows: • Credit Cards[34], Debit Cards[34], Reloadable Prepaid Cards

	Visa Acquirers	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction uses Visa Secure using EMV 3DS if it is assigned any of the following MCCs: • MCC 4722 (Travel Agencies and Tour Operators) • MCC 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls through Use of Magnetic Stripe Reading Telephones, and Fax Services) • MCC 5045 (Computers and Computer Peripheral Equipment and Software) • MCC 5310 (Discount Stores) • MCC 5722 (Household Appliance Stores) • MCC 5732 (Electronics Stores) • MCC 5734 (Computer Software Stores) • MCC 5941 (Sporting Goods Stores) • MCC 9402 (Postal Services – Government Only) Effective 15 October 2022 Ensure that its Electronic Commerce Merchant is enabled to process an Electronic Commerce Transaction using Visa Secure with EMV 3DS. If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Mainland China	**Visa Issuers**	An Issuer must ensure that its Visa Secure program provides a dynamic Authentication Mechanism to Cardholders such that the data elements used in one Transaction cannot be reused in another Transaction within a pre-defined time frame. An issuer that fails to comply with the dynamic authentication requirements in Mainland China will be subject to will be subject to a non-compliance assessment for each month of non-compliance
Philippines	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33]: • Credit Cards • Debit Cards

	Visa Acquirers	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following: MCCs: • MCC 3000-3350 (Airlines, Air Carriers) • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls through Use of Magnetic Stripe Reading Telephones, and Fax Services) • MCC 4900 (Utilities – Electric, Gas, Water, and Sanitary) • MCC 5331 (Variety Stores) • MCC 5999 (Miscellaneous and General Merchandise) • MCC 5499 (Miscellaneous Food Stores – Convenience Stores and Specialty Markets) • MCC 5722 (Household Appliance Stores) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Singapore	**Monetary Authority of Singapore (MAS), Technology Risk Management Guidelines**	Recommends that dynamic one-time password authentication be implemented for all card-not-present e-commerce transactions (Visa Secure meets this requirement).
	Visa Issuers	An Issuer must participate in Visa Secure with EMV 3DS[34]: • Credit Cards • Debit Cards

	Visa Acquirer	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS1 if it is assigned any of the following MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5815 (Digital Goods Media – Books, Movies, Music) • MCC 5816 (Digital Goods – Games) • MCC 5817 (Digital Goods – Applications [Excludes Games]) • MCC 5818 (Digital Goods – Large Digital Goods Merchant) • MCC 5968 (Direct Marketing – Continuity/Subscription Merchant) • MCC 8999 (Professional Services) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
South Korea	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[34]: • Credit Cards • Debit Cards
	Visa Acquirer	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following MCCs: • MCC 5968 (Direct Marketing – Continuity/Subscription Merchant) • MCC 5999 (Miscellaneous and Specialty Retail Stores) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Taiwan	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33], as follows: • Visa credit, Visa debit

	Visa Acquirers	Effective 16 January 2021 Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following MCCs: • MCC 4112 (Passenger Railways) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 7372 (Computer Programming, Data Processing, and Integrated Systems Design Services) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Thailand	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33]: • Credit Cards • Debit Cards
	Visa Acquirer	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS,1 if it is assigned any of the following MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5968 (Direct Marketing – Continuity/Subscription Merchant) • MCC 8999 (Professional Services) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Vietnam	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33]: • Credit Cards • Debit Cards
	Visa Acquirer	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with EMV 3DS, if it is assigned any of the following MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5311 (Department Stores) • MCC 7994 (Video Game Arcades/Establishments) If a Merchant is not enrolled in Visa Secure with EMV 3DS and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.

Canada		
Canada	**Visa Issuers**	Issuers that participate in Visa Secure must support Visa Secure for Visa Debit Category Cards. Effective 12 April 2025, all cards, except non-reloadable prepaid cards, are required to participate in Visa Secure at an ACS level. Issuers that participate in Visa Secure and support OTP (one-time passwords) via SMS and/or e-mail must be capable of sending "Informed OTP" which should include 1) the Merchant name and 2) Transaction amount. Issuers that participate in Visa Secure must be capable of supporting biometric authentication as one of the step-up challenge options for authenticating cardholders.
Central Europe Middle East and Africa		
All Countries	**Visa Acquirers**	Process Electronic Commerce Transactions using Visa Secure
	Visa Issuers	An Issuer that participates in Visa Secure must be capable of supporting risk-based authentication
Nigeria	**Visa Issuers**	Issuers must participate in Visa Secure for all products. Nigerian issuers must: • Complete the registration process for a ISO BIN before permitting a Cardholder to perform Electronic Commerce Transactions • Ensure that a Cardholder is enrolled in Visa Secure before authorizing Electronic Commerce • Authorize only a domestic Electronic Commerce Transaction for which the Acquirer has requested Visa Secure verification (except for Transactions processed under the International Airline Program)
	Visa Acquirers	Not process a domestic Electronic Commerce Transactions unless the cardholder has been successfully authenticated using Visa Secure

Europe		
All Countries	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS version 2.2, as follows: • Credit Cards, Debit Cards, Visa Commercial Cards Reloadable Prepaid Cards An Issuer that submits Secure Electronic Commerce Transactions must use Visa Secure. An Issuer must do all of the following: • Support a Visa-recognized payment Authentication Method • Notify its Cardholders of the availability of Visa-recognized payment Authentication Methods • Provide a Visa-recognized payment Authentication Method to a Cardholder upon Cardholder request • Monitor Electronic Commerce Transactions This requirement does not apply to Visa Commercial Cards and Cards bearing the Plus Symbol.
	Visa Acquirers	Process Secure Electronic Commerce Transactions using Visa Secure
Latin America		
Brazil	**Visa Issuers**	An Issuer must participate in Visa Secure with EMV 3DS[33]: • Debit Cards • Visa Electron Cards

B.2 ECI 6 Quality of Service Program

Issuers are not permitted to establish authorization processing criteria in which transactions that are submitted as attempted authentications (ECI 6) are blanket declined during authorization processing. This program is intended to manage authorization decline rates on ECI 6 transactions to help ensure a positive e-commerce experience for cardholders and protect the overall integrity of the Visa Secure.

B.2.1 Program Parameters

An Issuer that exceeds both 500 Authorizations a month and a decline rate of 50% or more for Transactions containing Electronic Commerce Indicator 6 (ECI 6) is subject to the non-compliance assessments specified in Table B-2, General Schedule of Non-Compliance Assessments – Tier 1.

The principles in Visa Europe differ from the ones provided here. Visa Europe issuers should contact their Visa representative for details.

For more information, see the *Visa Core Rules and Visa Product and Service Rules*.

Table B–2: General Schedule of Non-Compliance Assessments – Tier 1

Event	Visa Action/Non-Compliance Fee
Notification issued for violation of a rule	Warning letter with a request for a compliance/resolution plan
Response date has passed and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 25,000
30 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 50,000
60 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 75,000
90 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 150,000 Non-compliance assessments will continue to be levied each month until the rule violation is corrected, with the amount doubling each month.

B.3 Visa Secure Global Performance Enhancement Program

Visa Secure Global Performance Enhancement program defines issuer standards for "Authentication Failed" and "Unable to Authenticate" Authentication Responses to reduce excessive or inappropriate use of the "N", "R", and "U" status codes by issuers and protect the integrity of Visa Secure.

This appendix will describe the program rules for Issuer ACS on:

- Limits for "Authentication Failed" responses (EMV 3DS - ARes[35] = N or R, or RReq = N or R)
- Limits for "Unable to Authenticate" responses (EMV 3DS ARes = U or RReq = U)
- Out of Compliance Escalation Process

[35] Includes 3DS Requestor Initiated (3RI) transactions

B.3.1 Limits for "Authentication Failed" Responses

An Issuer whose ACS meets both of the following criteria is subject to conditions specified by the corresponding severity level:

- Exceeds 500 authentication transactions (i.e., ARes and RReq messages) for 2 consecutive months.
- **EMV 3DS**
  - Exceeds an ["N" + "R"] rate of 5.0% for 2 consecutive months:
    - The calculation for ["N" + "R"] transactions includes all eligible transactions in which the merchant genuinely and legitimately attempted to authenticate the cardholder.
    - The calculation is as follows:

      [(ARes=N or R) + (RReq=N or R)] / [(ARes=Y+N+A+U+R) + (RReq=Y+N+A+U+R)]

The actual rate determines the severity level and corresponding issuer and Visa actions to achieve compliance.

Table B–3: Global "N or R" Policy Requirements

Severity Level	["N" + "R"] Response Rate
Advice	5.0% to 7.49%
Alert/Warning	7.5% to 9.9%
Extreme Warning	10.0% and Above

B.3.2 Limits for "Unable to Authenticate" responses

An issuer responding to an authentication request with an Unable-to-Authenticate response (ARes = U or RReq = U) must do so only under one or more of the following conditions:

- Issuer experiences technical problems that prevent a timely response.
- Authentication data received from the merchant does not comply with the 3-D Secure specification.
- Transaction is attempted with a Non-Reloadable Visa Prepaid Card

An issuer whose ACS meets both of the following criteria is subject to conditions specified by the corresponding severity level:

- Exceeds 500 authentication transactions for 2 consecutive months.
- **EMV 3DS**
  - Exceeds an ["N" + "R"] rate of 5.0% for 2 consecutive months:
    - The calculation for ["N" + "R"] transactions includes all eligible transactions in which the merchant genuinely and legitimately attempted to authenticate the cardholder.

- The calculation is as follows:

  [(ARes=U) + (RReq=U)] / [(ARes=Y+N+A+U+R) + (RReq=Y+N+A+U+R)]

The actual rate determines the severity level and corresponding issuer and Visa actions to achieve compliance.

Table B–4: Global "U" Policy Requirements

Severity Level	"U" Response Rate
Advice	0.5 % to 0.99%
Alert/Warning	1.0 % to 1.24%
Extreme Warning	1.25% and Above

B.3.3 Out of Compliance Severity Levels

There are three levels of severity:

- Advice—"Advice" levels indicate that an issuer is sending higher-than-expected levels of "N" responses. Any actions taken (e.g., email notification that levels are higher than average) are at the discretion of Visa.
- Alert/Warning—"Alert/Warning" levels must be addressed by the issuer within 90 days of the initial report. The issuer may be required to provide Visa with transaction reports and a resolution plan to improve performance within 30 days of entering this status. Failure to do so will result in an automatic escalation to an Extreme Warning level.
  - In cases where an "Alert" is escalated to "Extreme Warning," the issuer must provide a resolution plan and implement the plan within 30 days of the escalation date.
- Extreme Warning—An issuer at the "Extreme Warning" level must provide to Visa a resolution plan within 60 days of the initial report (or when it enters the "Extreme Warning" level). The actions defined in the resolution plan must be implemented within 30 days of submission of the resolution plan.

B.3.4 Probation Period

Any issuer that has been notified under this program will remain on probation for a period of 6 months from the date of the initial report. At any time during this probation period, should the issuer revert to Alert or Extreme Warning status, it will immediately be escalated to Extreme Warning status, with 30 days to implement changes to address the situation. Failure to do so will result in escalation to Visa actions for non-compliance described in the following section.

B.3.5 Failure to Comply

Visa reserves the right to take the following actions when an issuer fails to comply with these terms,

- Stand in with "Attempts" functionality on behalf of the non-compliant issuer implementation, with the following terms:
  - Issuer will be subject to set-up fees and per-transaction fees related to the stand-in service
  - Issuer assumes liability for the resulting Attempts "A" transactions while it remains in stand-in status
  - Issuer will remain in this status until an agreement for resolution is reached with Visa
- Remove the non-compliant issuer implementation from the service by disconnecting it from the Visa Secure Directory Server, with the following terms:
  - Issuer assumes liability for the resulting transactions while it remains in non-participation status
  - Issuer will remain in this status until an agreement for resolution is reached with Visa
- Non-compliance assessments as specified in the *Visa Core Rules and Visa Product and Service Rules*.

C CAVV Verification Results Code (Field 44.13)

The CAVV Results Code (Field 44.13) identifies whether the CAVV value submitted in the authorization message passed or failed CAVV verification.

The issuer decides whether the issuer or VisaNet will perform CAVV verification during authorization for each participating ISO BIN/card range. During CAVV verification, the issuer's CAVV keys are used to verify the CAVV.

The CAVV Results Code augments other online risk management transaction data (e.g., Address Verification Value, CVV2, and Advance Authorization) and is available to the issuer at the time of authorization decisioning. Issuers are encouraged to develop an authorization strategy that utilizes a layered risk management approach.

For information about CAVV Results Codes and Values Descriptions, see the *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

D Acronyms and Glossary

D.1 Acronyms

This appendix provides a list of acronyms and a glossary of terms.

Acronym	Description
3DS	3-D Secure
AACS	Attempts Access Control Server
ACS	Access Control Server
BID	Business I.D.
AReq	Authentication Request
ARes	Authentication Response
ATN	Authentication Tracking Number
ISO BIN	**Issuer Bank Identification Number**
CAVV	Cardholder Authentication Verification Value
CReq	Challenge Request
CRes	Challenge Response
ECI	Electronic Commerce Indicator
NPA	Non-Payment Authentication
PCI DSS	Payment Card Industry Data Security Standard
PReq	Preparation Request Message
PRes	Preparation Response Message
RReq	Results Request Message
RRes	Results Response Message
SDK	Software Development Kit
TLS	Transport Layer Security
URL	Uniform Resource Locator

D.2 Glossary

Term	Definition
0-9	
3-D Secure (3DS)	The Three Domain Secure (3-D Secure™ or 3DS) Protocol has been developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance. EMVCo owns 3DS EMV 3DS. Visa's offering of 3DS is called Visa Secure.
3-D Secure Server (3DS Server)	A server or system that the merchant (or third party on the merchant's behalf) uses to support Visa Secure authentication processing.
3DS Server Client Certificate (3DSS Client Certificate)	The certificate used to secure the channel between the Visa Secure Directory Server and the 3DS Server when the Visa Secure Directory Server sends message to the 3DS Server.
3DS Server Server Certificate (3DSS Server Certificate)	The certificate used to secure the channel between the Visa Secure Directory Server and the 3DS Server when the 3DS Server sends message to the Visa Secure Directory Server.
3-D Secure Software Development Kit (3DS SDK)	A software component that is incorporated into the merchant's application to support Visa Secure processing on behalf of the 3DS Server.
3-D Secure Specification	A software protocol that enables secure processing of transactions over the Internet and other networks.
3DS Requestor	The initiator of the authentication request. For the scope of this document, this is the merchant.

Term	Definition
A	
Access Control Server (ACS)	A server hardware/software component that supports Visa Secure and other functions. The ACS is operated by the issuer or the issuer's processor. In response to Visa Secure Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the cardholder, and provides digitally signed authentication response messages (containing the authentication results and other Visa Secure data) to the merchant.
Acquirer	A member that signs a merchant or payment facilitator or disburses currency to a cardholder in a cash disbursement, and directly or indirectly enters the resulting transaction receipt into interchange.
Acquirer Identifier	A 6-digit number assigned by Visa that is used to identify an acquirer, VisaNet Processor, or Visa Scheme Processor for Authorization, Clearing, or Settlement processing.
ACS	See Access Control Server.
ACS Client Certificate	The certificate used to secure the channel between the Visa Secure Directory Server and the ACS when the Visa Directory Secure Server sends messages to the ACS.
ACS Operator ID	Visa-assigned ID that identifies the business entity operating the ACS.
ACS Server Certificate	The certificate used to secure the channel between the Visa Secure Directory Server and the ACS when the ACS sends messages to the Visa Secure Directory Server.
ACS Service Provider	The business entity operating an ACS or attempts server on behalf of the issuer.
ACS Signing Certificate	The certificate used to digitally sign authentication responses sent from the ACS to a Visa Secure merchant. Upon receipt, the merchant verifies the digital signature to ensure that the response was sent from an authorized ACS.

Term	Definition
Attempts Access Control Server (AACS)	A server hardware/software component that provides an attempted authentication response for issuers that do not have their own ACS. Like the ACS, the 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.
Attempts Response	A message from a Visa Secure issuer or an attempts service in response to an authentication request, indicating that the issuer or cardholder is not participating in Visa Secure.
Authentication	See cardholder authentication.
Authentication Data	All transaction-related data associated with a Visa Secure authentication request.
Authentication Request (AReq)	A EMV 3DS request for cardholder authentication from a Visa Secure merchant.
Authentication Response (ARes)	A EMV 3DS response from Visa Secure issuer, or Visa on behalf of an issuer, in response to an authentication request. Authentication responses include: • Attempt Responses • Unable-to-Authenticate Responses
Authenticated Payment Credential	A Payment Credential where the Issuer has confirmed the authenticity of the Payment Credential through Issuer identification and verification (ID&V) or Visa has determined the Payment Credential to have a sufficient history of successful Transactions at a registered Merchant such that the Issuer has effectively validated its authenticity, and the Payment Credential is uniquely associated with the registered Merchant or Token Requestor.
Authorization	A process where an issuer, a VisaNet processor, or stand-in processing approves a transaction. This includes offline authorization.
B	

Term	Definition
Issuing (ISO) Bank Identification Number (BIN)	A 6-digit identifier assigned by ISO to Visa and then licensed by Visa to an Issuer before 22 April 2022 and that comprises the first 6 digits of an Account Number. An 8-digit identifier assigned by ISO to Visa and then licensed by Visa to an Issuer and that comprises the first 8 digits of an Account Number.
Business ID (BID)	A unique Visa financial institution identification number assigned by Visa.
C	
Cardholder	An individual who is issued and authorized to use either or both a: • Card • Virtual Account
Cardholder Authentication	The process used to ensure that the transaction is being initiated by the rightful owner of the Visa account.
Cardholder Authentication Verification Value (CAVV)	A unique value transmitted in response to an authentication request that provides proof that authentication or attempted authentication took place on the transaction.
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 (CA)	An entity that issues and manages Digital Certificates for use with Visa products and services in accordance with Visa specified requirements. Entities eligible to be Certification Authorities within the Visa Certification Authority hierarchy include both: • Visa • Visa Members
Challenge Request (CReq) message	A EMV 3DS message sent by the 3DS SDK or 3DS Server where additional information is sent from the cardholder to the ACS to support the authentication process.

Term	Definition
Challenge Response (CRes) message	The ACS response to the EMV 3DS CReq message. It can indicate the result of the cardholder authentication or, in the case of a merchant application-based model, also signal that further cardholder interaction is required to complete the authentication.
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 (CSR)	Employees or agents who are responsible for primary customer support; can be employees of an issuer, acquirer or merchant.
D	
Digital Signature	A set of electronic data used to authenticate parties to a transaction.
Directory Server	See Visa Secure Directory Server.
Dynamic Password	See One-Time Passcode.
E	
Electronic Commerce Indicator (ECI)	A value used in an electronic commerce transaction to indicate the transaction's level of authentication and security.
F	
Failed Authentication	A message sent by a Visa Secure issuer in response to an authentication request that denies cardholder authentication. Also Authentication Failed or Not Authenticated.
I	
Interoperability Domain	The Visa operated systems in Visa Secure that connect the issuer and acquirer domains. See also Merchant/Acquirer Domain and Issuer Domain.
Issuer	A member that enters into a contractual relationship with a cardholder for the issuance of one or more card products.
Issuer Domain	The systems and functions of issuers and cardholders in Visa Secure. See also Merchant/Acquirer Domain and Interoperability Domain.

Term	Definition
Issuing Identifier	Assigned by Visa and used to define issuing processing. Multiple issuing (ISO) BINs may use the same issuing identifier
M	
Merchant	An entity that accepts a Visa Card for the sale of goods or services and submits the resulting transaction to an acquirer for interchange, directly or via a payment facilitator. A merchant may be a single merchant outlet or represent multiple merchant outlets.
Merchant/Acquirer Domain	The systems and functions of acquirers and merchants Visa Secure. See also Issuer Domain and Interoperability Domain.
Merchant Commerce Server	A server hardware/software entity that handles all online transactions and facilitates communication between the merchant application and the Visa gateway.
O	
One-Time Passcode	A one-time passcode is a Visa Secure cardholder authentication method. It is passcode that the issuer provides to the cardholder (usually via text or email) which can be used on one transaction to verify the identity of the cardholder.
P	
Payment Gateway	A third party that provides an interface between the merchant/acquirer's payment system and VisaNet.
Preparation Request (PReq) Message	The EMV 3DS PReq message is sent from the 3DS Server to the Visa Secure Directory Server to request information about the versions supported by available ACSs and, if one exists, any corresponding 3DS Method URL.
Preparation Response (PRes) Message	The EMV 3DS PRes message is the Visa Secure Directory Server response to the PReq message. The 3DS Server can utilize the PRes message to cache information about the versions supported by available ACSs, and if one exists, about the corresponding 3DS Method URL.
Proof of Attempted Authentication	See Attempts Functionality.
R	

Term	Definition
Results Request (RReq) message	An EMV 3DS message sent from the Issuer ACS to the 3DS Server via the Visa Secure Directory Server to transmit the results of the authentication transaction.
Results Response (RRes) message	The EMV 3DS 3DS Server response to the Results Result (RRes) message used to acknowledge receipt of this message.
Risk-Based Authentication	Risk-based authentication is a Visa Secure authentication approach. It may include analyzing historical data about the cardholder and merchant as well as taking into consideration the specifics of the transaction such as the amount or location. The risk profile is used to determine if authentication is successful, failed, or if step-up authentication (such as a one-time passcode) is required. See Step-up Authentication for additional information.
S	
Step-Up Authentication	When the issuer supports risk-based authentication and the results of authentication indicate that further authentication is required, the issuer can optionally request additional authentication from the cardholder such as a one-time passcode. This additional authentication method is referred to as step-up authentication.
T	
Technology Provider	An entity that provides technical services in support of Visa Secure.
Three-Domain Secure	See 3-D Secure.
Transport Layer Security (TLS)	A protocol that is designed to secure processing of transactions over the internet and other networks.
U	
Unable-to-Authenticate Response	A message from a Visa Secure Issuer in response to an authentication request indicating that the issuer is unable to authenticate the cardholder for reasons other than those that result in an authentication denial.
Uniform Resource Locator (URL)	Global address used for locating resources on the Internet.
V	

Term	Definition
Visa Secure Directory Server	A server hardware/software entity that is operated by Visa, whose primary function is to route authentication requests from merchants to specific ACSs and to return the results of authentication.
Visa Method URL	A 3DS Method URL capability provided by Visa and any sub-processors, on behalf of Visa Secure Issuer clients who do not currently provide their own 3DS Method URL capability. It is invoked by 3DS Requestors for 3-D Secure browser authentication transactions as defined in the EMV 3-D Secure specification and allows for the capture of additional browser and device information to help facilitate transaction risk assessment.
Visa Secure	Visa's implementation of the 3-D Secure & EMV 3DS protocols.
Visa Secure On-Behalf-Of-Issuer Services	An opt-in service designed to improve authentication and authorization for Visa B2B Virtual Card account and Visa Pseudo Account transactions on behalf of issuers.
VisaNet	The systems and services, including the V.I.P. System, Visa Europe Authorization Service, and BASE II, through which Visa delivers online financial processing, authorization, clearing, and settlement services to members, as applicable.