



Mastercard Identity Check Program Guide

19 November 2019

Contents

Summary of Changes, 19 November, 2019.....	7
Chapter 1: Mastercard Identity Check Introduction.....	13
EMV 3-D Secure.....	14
Mastercard Identity Check Program.....	14
Anonymous Prepaid Cards.....	15
Why Mastercard Identity Check.....	15
Audience and Scope.....	16
Program Participant Impact.....	16
Terminology.....	17
Related Documentation.....	17
Contact Information.....	19
Chapter 2: Mastercard Identity Check Program.....	20
How Identity Check Uses EMV 3-D Secure Protocol.....	21
Mastercard Identity Check Ecosystem.....	22
How Mastercard Identity Check Works and Core Functionality.....	26
3-Domain Model.....	26
Directory Server and Smart Authentication Services.....	27
Smart Authentication Stand-In.....	27
Smart Authentication for ACS/Issuers.....	29
Digital Transaction Insights (DTI).....	30
Message Types.....	32
Mastercard Identity Check Use Cases.....	33
Additional Features.....	35
Identity Check Insights.....	35
Identity Check Insights Process and Technical Readiness	35
Acquirer Strong Consumer Authentication (SCA) Exemption.....	36
Merchant Fraud Rate.....	40
Acquirer Country Code.....	41
Merchant Whitelisting.....	42
Whitelisting Request during Authentication Transaction.....	43
Whitelisting Status Response.....	44
Whitelist Exemption.....	46
Whitelist Status Check.....	47
AAV Refresh	48
Mastercard On-behalf AAV Validation Service	50

Chapter 3: Mastercard Identity Check Global Program

Requirements.....	52
Mastercard Identity Check Engagement Requirements.....	54
Approved Methods for Authentication.....	56
Authentication Methods Not Allowed.....	59
Authentication Experience Requirements.....	60
User Interface Requirements for App-based Transaction Flows.....	61
Key Performance Indicators—Compliance Measures.....	62
Privacy and Data Protection Matters.....	64
Requirements for Authentication Method.....	72
Risk Based Authentication.....	73
Biometric Authentication.....	74
Biometric—Fingerprint Match.....	74
Biometric—Facial Recognition.....	75
Biometric—Voice Recognition.....	75
Interactive Cards with PIN Pads.....	76
Push Notification Requesting Transaction Approval.....	76
Hand-held Token Generators/Fobs.....	77
One-Time Passcode through SMS.....	78
One-Time Passcode through Mobile App.....	78
Issuer Portal Verification.....	79
Fallback Method Using Email.....	79
Payment Transactions.....	81
Regular e-Commerce Payment Transaction	81
3RI Payments	81
Delayed Delivery/Charged.....	82
Partial Split Shipment	82
Payment Initiated by a Different Merchant.....	83
Agent Payment (with Multiple Merchants)	83
Unknown and Undefined Final Amount before Purchase.....	84
Installment Payments.....	85
Refund of a Purchase	86
Replacement (Re-authorization) of a Refunded Purchase	86
Adding Card-on-File—Regular Payment.....	87
Adding Card-on-File—Recurring Payment.....	87
Mail Order / Telephone Order (MOTO).....	88
Recurring Payments.....	88
Recurring Payment with Fixed Amounts	92
Recurring Payment with Variable Amounts	92
Recurring Payment Combined with One-time Purchase.....	93
Recurring Payment with Fixed Limit and Threshold	94

Use of Account Status Inquiry (ASI) in Recurring Payment.....	94
Non-Payment Transactions.....	95
Chapter 4: Liability Shift and Processing Matrix.....	97
Liability Shift Rule Summary.....	98
Transaction Processing Matrix.....	98
Accessing the Processing Matrix File.....	99
Mastercard Identity Check Transaction Processing Requirements.....	100
Mastercard Identity Check Required Data Elements.....	105
Chapter 5: Identity Check Regional Program Requirements - EU.....	112
Privacy and Data Protection – Europe.....	113
Revised Payment Service Directive (PSD2) Requirements.....	119
Strong Customer Authentication.....	119
Soft Decline or Decline as SCA Required	119
PSD2 SCA Exemptions and Maestro	120
Dynamic Linking.....	120
Biometric Authentication Support.....	121
Auto-enrollment.....	122
Mandated Support for EMV 3-D Secure.....	122
Acquirer Strong Consumer Authentication (SCA) Exemption	122
Low-Value Payments and Management of Counters.....	124
Merchant Fraud Rate.....	124
Acquirer Country Code.....	124
Secure Corporate Payments Exemptions	125
Merchant Whitelisting.....	126
Recurring Payments/MITs.....	127
Mastercard Services in Support of PSD2 RTS	128
Mastercard On-Behalf AAV Validation Service.....	128
Authentication Express (Europe).....	128
Appendix A: Mastercard Authentication Best Practices.....	129
Authentication Best Practices Introduction.....	130
Definition of Strong Authentication.....	130
Interpreting the Three Factors for Strong Authentication.....	131
Best Practices for Enhancing Consumer Experience.....	134
Authentication Methods not Allowed with Identity Check.....	137
Appendix B: Branding Guidelines.....	138
Mastercard Identity Check Identifier.....	139

Appendix C: Digital Transaction Insights.....	140
Risk Levels 0-9.....	141
Reason Code Approach.....	141
Reason Codes.....	143
Appendix D: Merchant Data Message Extension.....	147
Merchant Data.....	148
Appendix E: ACS Data Message Extension.....	151
ACS Data.....	152
Appendix F: Payment Transaction Flow (Version 2.1 and 2.2)	154
Payment Transaction Flow (Both Versions)	155
Appendix G: Non-Payment Transaction Flow (Version 2.1 and 2.2)....	157
Non-Payment Transaction Flow (Both Versions)	158
Appendix H: BIN Table Resource	160
BIN Table Resource.....	161
Appendix I: Identity Check Insights – Sample Responses	162
Identity Check Insights – Sample Success Responses	163
Identity Check Insights – Sample Failed Response	163
Appendix J: Regular E-commerce Payment Transaction— Authorization Data Elements	165
Authorization Data Elements.....	166
Appendix K: Recurring Payment Transaction—Authorization Data Elements	171
Authorization Data Elements	172
Appendix L: Transaction Status, SLI, and Liability Mapping.....	179
Transaction Status.....	180

Appendix M: 3RI Payment Transaction Flow	181
3RI Payment Transaction Flow for Version 2.2	182
Appendix N: Mastercard Identity Check Insights Transaction Flow	183
Identity Check Insights Transaction Flow.....	184
Appendix O: Security Measures.....	185
Security Measures Types.....	186
Appendix P: Acronyms.....	188
Notices.....	198

Summary of Changes, 19 November, 2019

This document reflects changes effective since the last publication of this manual.

Description of Change	Where to Look
Minor editorial, grammar, typographic fixes, or formatting changes.	Throughout
Change term: “Stand In” to “Smart Authentication Stand-In”	
Update images to change terms.	
Change term: “aggregator” to “agent”	
Change term: “Data Only” to “Identity Check Insights”	
Update and add multiple Requirement numbers	
Change term, “Stand-In Risk-Based Authentication (RBA)” to “Smart Authentication Stand-In”.	
Change term, “Access Control Server Risk Based Authentication (ACS RBA)” to “Smart Authentication for ACS/Issuers”.	
Chapter 1 Mastercard Identity Check Introduction	
Update topic	Related Documentation
Merge <i>Program Onboarding and Implementation</i> topic into Related Documentation section.	
Chapter 2 Mastercard Identity Check Program	
Update topic and sub topics	Directory Server and Smart Authentication Services
Update topic; content and title from “Directory Server and Risk Based Authentication Services” to “Directory Server and Smart Authentication Services”.	Directory Server and Smart Authentication Services
	Recurring Payments/MITs
Requirement 121 moved from Chapter 4 to Chapter 2 <i>Recurring Payments/MITs</i> .	Smart Authentication for ACS/Issuers

Description of Change	Where to Look
Add sub topics to: “ <i>How Mastercard Identity Check Works and Core Functionality</i> ” topic.	Additional Features Identity Check Insights Identity Check Insights Process and Technical Readiness Data Only Transaction Processing Acquirer Strong Consumer Authentication (SCA) Exemption Merchant Fraud Rate Acquirer Country Code Merchant Whitelisting Whitelisting Request during Authentication Transaction Whitelisting Status Response Whitelist Exemption Whitelist Status Check AAV Refresh Mastercard On-behalf AAV Validation Service
Delete sub topic under <i>Additional Features</i>	<i>Data Only Transaction Processing</i> section
Chapter 3 Mastercard Identity Check Global Program Requirements	
Update topics Changed topic title from: “Support of Multiple Device Types Requirements” to “Authentication Experience Requirements”	Authentication Experience Requirements Key Performance Indicators—Compliance Measures Requirements for Authentication Method Biometric—Fingerprint Match Biometric—Facial Recognition Biometric—Voice Recognition Issuer Portal Verification Fallback Method Using Email Adding Card-on-File—Recurring Payment Non-Payment Transactions

Description of Change	Where to Look
Add topics	Regular e-Commerce Payment Transaction 3RI Payments Delayed Delivery/Charged Partial Split Shipment Agent Payment (with Multiple Merchants) Unknown and Undefined Final Amount before Purchase Installment Payments Refund of a Purchase Replacement (Re-authorization) of a Refunded Purchase Regular e-Commerce Payment Transaction Adding Card-on-File—Regular Payment Mail Order / Telephone Order (MOTO) Adding Card-on-File—Recurring Payment Recurring Payment with Fixed Amounts Recurring Payment with Variable Amounts Recurring Payment Combined with One-time Purchase Recurring Payment with Fixed Amounts Biometric Authentication Use of Account Status Inquiry (ASI) in Recurring Payment
Delete topics Delete topic title “Merchant and 3DS Server Specifications” and moved table to “Authentication Experience Requirements”	
Chapter 4 Liability Shift and Processing Matrix	
Update topics and sub topics	Liability Shift Rule Summary Transaction Processing Matrix Accessing the Processing Matrix File Mastercard Identity Check Transaction Processing Requirements
Chapter 5 Identity Check Regional Program Requirements - EU	

Description of Change	Where to Look
Update topics and all sub topics	Revised Payment Service Directive (PSD2) Requirements Strong Customer Authentication Soft Decline or Decline as SCA Required Dynamic Linking Biometric Authentication Support Auto-enrollment Mandated Support for EMV 3-D Secure Acquirer Strong Consumer Authentication (SCA) Exemption Low-Value Payments and Management of Counters Merchant Fraud Rate Acquirer Country Code Secure Corporate Payments Exemptions Merchant Whitelisting Recurring Payments/MITs Anonymous Prepaid Cards Mastercard On-Behalf AAV Validation Service Authentication Express (Europe)
Add topics and sub topics.	Privacy and Data Protection – Europe Mandated Support for EMV 3-D Secure Acquirer Strong Consumer Authentication (SCA) Exemption
Delete topics <ul style="list-style-type: none"> • Mail Order / Telephone Order (MOTO) • One-leg Transactions • Merchant Initiated Transaction 	
Appendices	

Description of Change	Where to Look
<p>Delete the below and update all Appendix letters.</p> <p>Appendix C-Mastercard Digital Security Road Map for Europe</p> <p>Appendix D-Reference Announcements for All Countries in Europe</p> <p>Appendix Q Smart Authentication Stand-In Service</p>	
<p>Added during the 20 November 2018 version update, yet was not on the Summary of Changes for that version = Appendix E-Digital Transaction Insights.</p> <p>Update: Appendix E now Appendix C-Digital Transaction Insights.</p>	<p>Digital Transaction Insights</p>
<p>Merge original appendices into Appendix F-Payment Transaction Flow (Version 2.1 and 2.2)</p> <ul style="list-style-type: none"> • Appendix H-Payment Transaction Flow (Version 2.1) • Appendix I-Payment Transaction Flow (Version 2.2) <p>Original Appendix I is now Appendix G-Non-Payment Transaction Flow (Version 2.1 and 2.2).</p>	<p>Payment Transaction Flow (Version 2.1 and 2.2)</p> <p>Non-Payment Transaction Flow (Version 2.1 and 2.2)</p>
<p>Merge original appendices into Appendix I-Identity Check Insights - Sample Responses</p> <ul style="list-style-type: none"> • Appendix K-Data Only - Sample Success Response • Appendix L-Data Only - Sample Failure Response 	<p>Identity Check Insights – Sample Responses</p>
<p>Update Appendix F is now Appendix D-Merchant Data Message Extension</p>	<p>Merchant Data Message Extension</p>
<p>Update Appendix G is now Appendix E-ACS Data Message Extension</p>	<p>ACS Data Message Extension</p>
<p>Update Appendix J is now Appendix H-BIN Table Resource</p>	<p>BIN Table Resource</p>
<p>Add Appendix J-Regular E-commerce Payment Transaction—Authorization Data Elements</p>	<p>Regular E-commerce Payment Transaction—Authorization Data Elements</p>
<p>Add Appendix K-Recurring Payment Transaction—Authorization Data Elements</p>	<p>Recurring Payment Transaction—Authorization Data Elements</p>

Description of Change	Where to Look
Add Appendix L-Transaction Status, SLI, and Liability Mapping	Transaction Status, SLI, and Liability Mapping
Add Appendix M-3RI Payment Transaction Flow	3RI Payment Transaction Flow
Add Appendix N-Mastercard Identity Check Insights Transaction Flow	Mastercard Identity Check Insights Transaction Flow
Add Appendix O-Security Measures	Security Measures
Add Appendix P-Acronyms	Acronyms

Chapter 1 Mastercard Identity Check Introduction

This section describes the Mastercard authentication program known as Mastercard Identity Check™, aimed at providing an optimized consumer experience.

EMV 3-D Secure.....	14
Mastercard Identity Check Program.....	14
Anonymous Prepaid Cards.....	15
Why Mastercard Identity Check.....	15
Audience and Scope.....	16
Program Participant Impact.....	16
Terminology.....	17
Related Documentation.....	17
Contact Information.....	19

EMV 3-D Secure

EMV® 3-D Secure (sometimes referred to herein as EMV 3DS) supports secure e-commerce transactions.

The world is rapidly moving to digital payments. The approval rates in digital remain lower than the physical world and fraud is on an incline. Payments in the digital world need to be safe and simple.

To meet this current and future need for better and safe authentication; EMVCo evolved the EMV specification and created the EMV 3-D Secure specification that supports secure e-commerce transactions in a globally interoperable manner. The specification supports not only traditional browser-based e-commerce transactions, but also app-based authentication, integration with digital wallets, and non-payment authentication.

Benefits of EMV 3-D Secure

- Improved consumer experience – integrated into checkout experience
- Improved performance of payment authentication flows
- Supports a device agnostic approach – including app based flows
- Richer data set allows for better communication of data between merchants and issuers
- Supports frictionless authentication (Risk-Based) and low friction challenge such as biometrics
- Non-Payment Authentication flow added to support functions like adding a card to a wallet or cardholder verification as part of the tokenization process

Mastercard Identity Check Program

The Mastercard Identity Check™ program is a global authentication program that builds upon the existing Mastercard SecureCode™ program and uses the current EMV® 3-D Secure protocol.

Mastercard Identity Check is designed to help provide additional security for digital transactions and facilitate higher approval rates, by improving the authentication experience for merchants, issuers, and cardholders for e-commerce transactions. The program focuses on state of the art, user-friendly verification methods; and couples those methods with key performance indicators to ensure that fraud levels remain in check and consumer experience is optimal.

Registrants of Mastercard Identity Check Program

Issuers, acquirers, Access Control Server (ACS) providers, and 3-D Secure servers (each a “Registrant”) can register for and participate in the Identity Check Program if they agree to the Identity Check Program Registration Terms and Conditions using the Mastercard Identity Check Test Platform on Mastercard Connect, and meet the requirements set forth in this Program Guide.

If a Registrant is enrolling other participating entities (including but not limited to merchants, processors or gateways) into the Identity Check Program, (a) Registrant is authorized by such participating entities to enroll them into the Identity Check Program, (b) each participating entity has been provided with, understands, and has agreed to comply with this Program Guide, and (c) Registrant is fully responsible for such participating entities' participation in the Identity Check Program.

NOTE: Mastercard Identity Check program requirements are valid for all Mastercard Credit and Debit cards (consumer or commercial.) Private label (PVL) closed network cards are excluded from our network requirements as well as PSD2 RTS as these follow their own PVL rules instead of Mastercard rules.

Anonymous Prepaid Cards

Currently, payments made through the use of anonymous payment instruments, such as anonymous prepaid (for example, gift) cards, are not subject to the Identity Check program requirements; therefore, do not have to be enrolled in the program. Some issuers may still consider enrolling these cards.

There are no specific Mastercard product code, or Mastercard BINs associated with the anonymous payment instruments. Acquirers cannot identify an anonymous prepaid card from the primary account number. These types of cards are only identified or known by the issuer.

Mastercard is introducing a new account range indicator ("Anonymous indicator") in its core network (authorization and clearing) which indicates to acquirers whether a Mastercard and Maestro™ prepaid account range is anonymous or non-anonymous.

For more information on this topic, refer to the following announcement *AN 2625—Identification of Anonymous Prepaid Cards*.

Payments made through the use of anonymous payment instruments, such as anonymous prepaid (for example, gift) cards, are not subject to the Identity Check program requirements; therefore, do not have to be enrolled in the program. Some issuers may still consider enrolling these cards due to the concern that, if they do not, the authentication request will result in attempts processing (with lower approval rate) which in turn may lead to merchants not accepting this payment form for their e-commerce business.

Why Mastercard Identity Check

Preventing fraud for Card Not Present (CNP) transactions has been a concern for several years.

Methods for authentication that are widely used are very intrusive or cumbersome for cardholders, which has led to high abandonment rates at merchants.

The Mastercard Identity Check™ program replaces static passwords, burdensome security questions, and other such methods with risk-based authentication, single use codes, biometrics, and other next-generation solutions. These methods leverage advanced technology to provide cardholders with simple and secure authentication that makes it easy and safe to shop online.

Audience and Scope

The Mastercard Identity Check™ Program Guide is a reference for both prospective and current Identity Check Program Participants.

The term 'Program Participant' used in this documents includes Registrants (defined above) as well as other participating entities (including but not limited to merchants, processors and gateways), who want to implement or make changes to their existing implementation of the Identity Check Program.

All Identity Check Program Participants are subject to the terms and conditions set forth in the Identity Check Test Platform as well as all other Identity Check documentation. Refer to Chapter 2 of this document for roles and responsibilities of the various Program Participants.

This Program Guide includes overviews, as well as detailed information, on the program services, program requirements, and processing requirements. This guide and all program materials are subject to change. Mastercard has the right, in its sole discretion, to interpret, amend, and enforce this and other guides, and all other Mastercard Standards.

For questions regarding this guide, contact Mastercard Customer Technical Support (CTS) or email IDC_Customer_Support@mastercard.com.

Program Participant Impact

The Mastercard Identity Check™ authentication program is the next generation program with its origin from Mastercard SecureCode™.

The same transaction liability structure, interchange program rates and fees, and authorization and clearing indicators apply to both authentication programs. For example, all existing SecureCode liability shifts will also apply to the use of Identity Check. The Mastercard Identity Check program rules will be incremental to the existing SecureCode rules provided in the *Mastercard Rules*, *Chargeback Guide*, and *Transaction Processing Rules*.

Many issuers may already have authentication solutions that meet the qualifications for the Identity Check program. Issuers should work with their Access Control Servers (ACS) to review their best options for Identity Check program participation. Merchants also need to work with their payment gateways, 3-D Secure Server providers and acquirers to ensure best in class solutions.

Terminology

Mastercard Identity Check™ Program uses the following words in this guide that have a specific meaning. These match with terminology used in the EMV® 3-D Secure specifications.


Term	Definition
Shall	Defines a product or system capability, which is mandatory.
Must	Defines a product or system capability which is mandatory.
May	Defines a product or system capability, which is optional or a statement which is informative only and is out of scope for this specification.
Should	Defines a product or system capability, which is recommended.

Related Documentation

Program Registrants can obtain supporting documentation through the following means.

Accessing Publications

Refer to the following documents available on [Mastercard Connect](#).

To select desired applications, go to **Store** (for example **Technical Resource Center** or the **Publications** applications). Select the  image on the application as a favorite. Favorite applications are stored in the **My Items** tab.

Find and click **Publications** application and search for a related publication below.

Program Onboarding and Implementation, and other Reference Materials

This section contains details of how to onboard and implement the Mastercard Identity Check™ program. Find these details in the onboarding guides and other reference materials, which are available on Mastercard Connect > Publications.

- *Mastercard ACS Compliance Program*
- *Mastercard 3DSS Compliance Program*
- *Mastercard Identity Check Onboarding Guide for 3-D Secure Acquirers, Merchants, and Service Providers*

- *Mastercard Identity Check Onboarding Guide for ACS Service Providers, Operators, Issuers, and Processors*
- *Mastercard Identity Check Test Platform User Guide*
- *Mastercard Identity Solutions Services Management User Guide*
- *SPA2 AAV for Mastercard Identity Check Program*
- *IPM Clearing Formats*
- *Identity Check ACS RBA Service*
- *Authentication Guidelines for Europe*
- *Transaction Processing Rules*
- *Mastercard Rules*
- *Authentication Guide*
- *Announcement AN 2723*
- *Authentication Express Program Guide*
- *Customer Interface Specification Chargebacks Guide*

Other Reference Materials

Mastercard Standards for Merchant Whitelisting

Accessing Announcements (Bulletins)

Favorite applications are stored in the **My Items** tab. In the My Items, type in the search field = **Announcements** and then click the **Technical Resource Center** application.

Click **Announcements** tab to browse for the latest Announcements on Mastercard Identity Check™ Program using the **Search Topics** and **Filters**.

Refer to Mastercard Connect, URL: <https://www.mastercardconnect.com/business/public/en-us/public/signin.html>.

Helpful Links

Refer to the following links:

- To manage your company's contacts: My Company Manager (link 'My Company Manager' to Mastercard Connect URL:
- Mastercard Brand Center URL: <https://brand.mastercard.com/brandcenter.html>
- Mastercard Identity Check Vendor List, URL: <https://www.mastercard.us/en-us/merchants/safety-security/securecode/securecode-vendors.html>
- 2.0 Qualtric Upload link is URL: https://mastercard.azure.com/qualtrics.com/jfe/form/SV_41tJYjsidllxC5
- EMV® 3-DS Specifications and other related technical documentation, refer to URL: <https://www.emvco.com/>
- EMVCo Certified Service Providers at URL: <https://www.emvco.com>.

Contact Information

Program Participants can reach Mastercard Global Customer Technical Support (CTS) for support through the following means.

Business hours

Monday through Friday
08:00 CST - 17:00 CST

Phone: 1-636-722-6176
Toll-free 1-800-999-0363

Email: IDC_Customer_Support@mastercard.com

After Hours, Weekend and Holidays; Support for Critical Issues only*

Operations Command Center (OCC) Escalations

Phone

Toll-free 800-358-3060 or +1 636 722 6220

COS Escalation email address

OCC@mastercard.com

IDC compliance related matters email address

identity_solutions_compliance@mastercard.com

*Critical Issues include

- Fatal errors and substantive data loss has occurred
- Issue has a substantial impact on multiple customers, users, or companies
- A major component of the system is not available

Customer Implementation Services

Email

All regions, Asia/Pacific, Canada and U.S., Europe, Latin America and the Caribbean, and Middle East/Africa, should use the below email for the Customer Implementation Services (CIS) contact.

Identity_Check_Mandate_Testing@mastercard.com

Chapter 2 Mastercard Identity Check Program

Mastercard Identity Check™ Program, is the next generation of digital authentication and like other critical security solutions, Identity Check operates on industry standard - EMV® 3-D Secure.

How Identity Check Uses EMV 3-D Secure Protocol.....	21
Mastercard Identity Check Ecosystem.....	22
How Mastercard Identity Check Works and Core Functionality.....	26
3-Domain Model.....	26
Directory Server and Smart Authentication Services.....	27
Smart Authentication Stand-In.....	27
Smart Authentication for ACS/Issuers.....	29
Digital Transaction Insights (DTI).....	30
Message Types.....	32
Mastercard Identity Check Use Cases.....	33
Additional Features.....	35
Identity Check Insights.....	35
Identity Check Insights Process and Technical Readiness	35
Acquirer Strong Consumer Authentication (SCA) Exemption.....	36
Merchant Fraud Rate.....	40
Acquirer Country Code.....	41
Merchant Whitelisting.....	42
Whitelisting Request during Authentication Transaction.....	43
Whitelisting Status Response.....	44
Whitelist Exemption.....	46
Whitelist Status Check.....	47
AAV Refresh	48
Mastercard On-behalf AAV Validation Service	50

How Identity Check Uses EMV 3-D Secure Protocol

EMV® 3-D Secure allows for an enhanced consumer authentication approach for greater security. Richer data and greater security allows for a stronger risk-based authentication experience and decisioning.

Whenever possible, Mastercard Identity Check™ recommends a risk-based authentication approach so that it can help authenticate consumers without friction in most Card Not Present (CNP) transactions, thereby offering a consistent experience.

The challenge or step-up authentication methods can be used in regulated markets or where the issuer feels the need for additional security. A dynamic step-up authentication method is required, instead of static methods. The list of Mastercard-approved authentication methods can be found in the Program Requirements section of this guide.

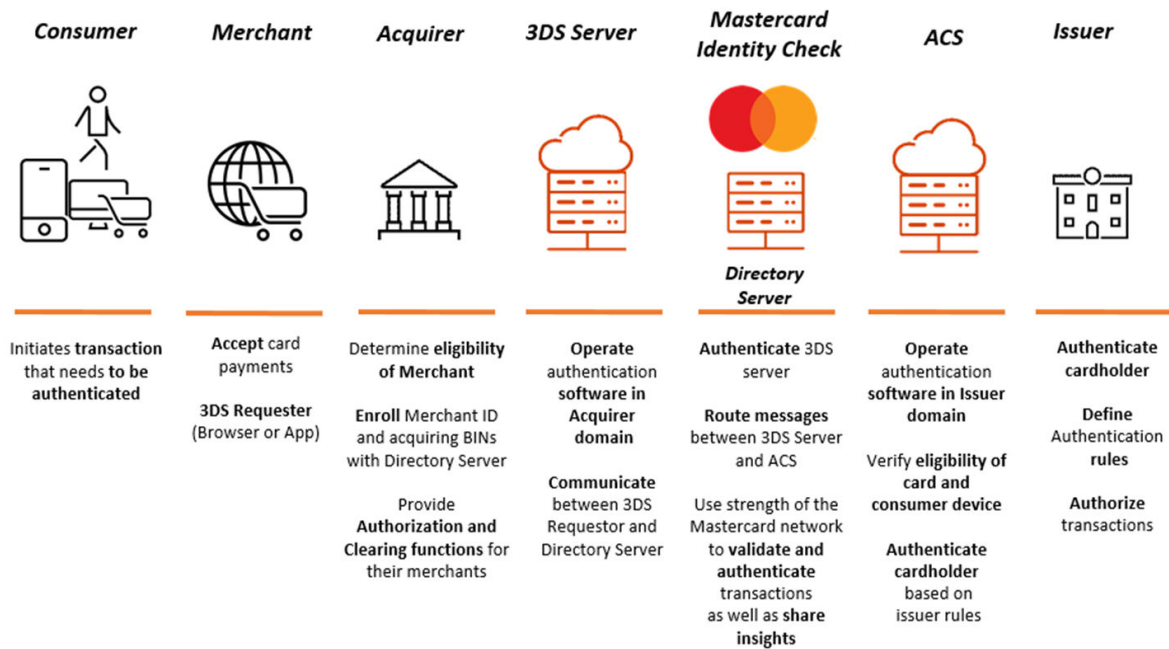
NOTE: Identity Check program requirements are valid for all Mastercard Credit and Debit cards (consumer and commercial). Payments made through the use of anonymous payment instruments, such as anonymous prepaid (for example, gift) cards, are not subject to the Identity Check program requirements. Private label (PVL) closed network cards are excluded from our mandates as well as PSD2 RTS as these follow their own PVL rules instead of Mastercard rules.

Mastercard Identity Check Ecosystem

The Mastercard Identity Check™ ecosystem includes several stakeholders. The descriptions, roles, and benefits for the stakeholders, are identified below.

Stakeholders

Mastercard Identity Check™ Ecosystem



Roles

The table below describes the roles played by each of the stakeholder of the ecosystem. All the Identity Check Program Participants must adhere to the Identity Check Program Requirements as set forth in this guide.

Stakeholder	Role Description
Cardholder	An individual who has been issued a Mastercard card and is authorized to use it at a merchant website or application for e-commerce transactions.

Stakeholder	Role Description
Issuer	<ul style="list-style-type: none"> • A principal customer of Mastercard, licensed by Mastercard to offer branded products and services. • An Identity Check Program Participant, is responsible for enrolling card ranges eligible to participate in Identity Check with Mastercard Directory Server. • Authenticate cardholder. • Own or work with issuer Access Control Server (ACS) on authentication needs and define authentication rules. • Pass the Issuer Authentication Value (IAV) for each authenticated transaction. • Make decisions on transactions authorization based on authorization messages received from acquirers through Mastercard Authorization system (Banknet/MDS). • Referred to as a “Hosted Principal” customer if they use a service hosted by a third party ACS.
Access Control Server (ACS)	<ul style="list-style-type: none"> • An Identity Check Program Participant, is responsible for operating authentication software in issuer domain. • Verify eligibility of a card and consumer device for Identity Check authentication. • Authenticate cardholder based on rules set by the issuer. • Pass the Issuer Authentication Value (IAV) for each authenticated transaction.
Merchant	<ul style="list-style-type: none"> • An Identity Check Program Participant, is responsible for integrating with acquirer or payment service providers to accept card payments for goods or services they sell through a website or application. • Own or work with 3-D Secure Server for authentication needs. • Act as 3-D Secure service requestor that is using authentication services from a 3-D Secure server. The 3-D Secure requestor may use a 3-D Secure SDK.

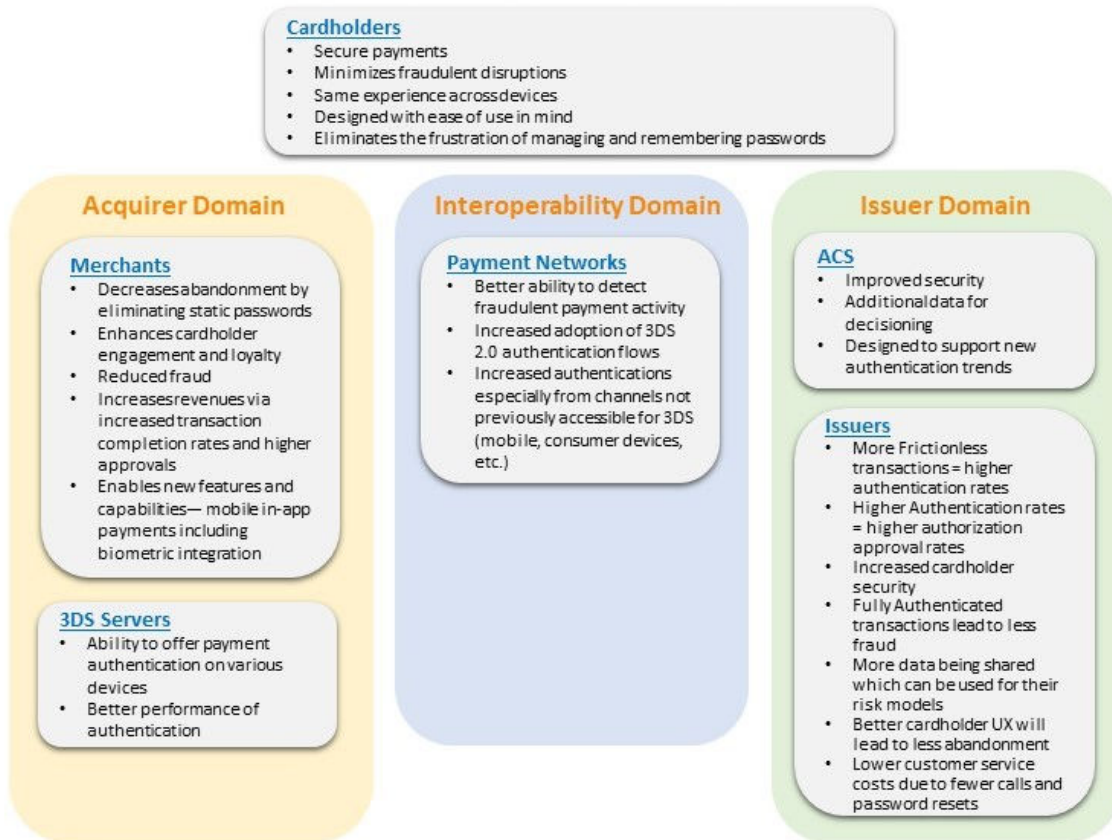
Stakeholder	Role Description
Acquirer	<ul style="list-style-type: none"> • A principal customer licensed by Mastercard to offer branded products and services. • An Identity Check Program Participant, is responsible for determining eligibility of merchant to participate in Identity Check program. • Enrollment and management of registered merchants on the Directory Server. • Provides the authorization and clearing functions for their merchants utilizing Mastercard Identity Check Program. • Format and send authorization messages to issuer for decision by way of Mastercard Authorization system (Banknet/MDS), and forwards decision to merchant. • Receives authorization decisions from issuers and sends to merchants. • Send completed transactions to Mastercard clearing system (GCMS). • Referred to as a “Hosted Principal” customer if they use a service hosted by a third party 3-D Secure Server solution.
Processor	<p>An Identity Check Program Participant, is responsible for managing Mastercard activities for Mastercard principal customers.</p>
3-D Secure Server	<ul style="list-style-type: none"> • An Identity Check Program Participant, is responsible for operating authentication software in Acquirer domain. • Communicate between 3-D Secure requestor and Directory Server and ensure messaging is secure.
Directory Server	<ul style="list-style-type: none"> • An Identity Check Program Participant, is responsible for operating in Interoperability domain. • Authenticates the 3-D Secure Server and routes messages between 3-D Secure Server and ACS. • Communicates with Mastercard Decision Management Platform (DMP) and Mastercard Smart Authentication services which offer the capability to stand-in with risk based authentication on behalf of the issuer in certain pre-defined scenarios.

Stakeholder	Role Description
Mastercard	<ul style="list-style-type: none">• Manages Mastercard Identity Check program compliance.• Manages 3-D Secure Service provider program.• Provides the Mastercard Identity Check testing platform.• Assigns 3-D Secure Server Operator ID and generates a letter of completion.• Provides Smart Authentication services and additional authentication features for greater experience.• Provides certificates for connectivity.• Provides access to publications.• Provides the authentication network and the Mastercard Identity Check Directory Server to connect merchants to issuers/cardholders.

Benefits

Mastercard Identity Check key benefits to its Program Participants by role are shown below:

Mastercard Identity Check™ - Benefits to Stakeholders



How Mastercard Identity Check Works and Core Functionality

This section demonstrates the interaction between three domains (acquirer, interoperability, and issuer), the Mastercard Directory Server (DS)™, and the scoring model.

3-Domain Model

The Mastercard Identity Check™ Program operates on the core concept of three domains of the EMV® 3-D Secure specification.

Those domains are:

- Acquirer Domain – this is where transactions are initiated

- Interoperability Domain – this is where transactions are switched between acquirer and issuer domain
- Issuer Domain – this is where transactions are authenticated

NOTE: For more details on the 3-Domain Model, refer to *EMV 3-D Secure Core Specification*.

Directory Server and Smart Authentication Services

The Mastercard Directory Server™ (DS) operates in the Interoperability Domain and offers a robust authentication risk assessment and decisioning platform.

The additional data in the EMV® 3-D Secure message construct and support for increased data exchange between the merchant and the issuer enables expansion of risk-based authentication (RBA) decisioning. RBA allows an issuer to examine every authentication request through transaction risk analysis, but focus their fraud prevention efforts on the transactions that present the most risk. RBA uses behavioral and transactional inputs in conjunction with a risk engine to determine riskiness of the authenticating transaction.

Mastercard has developed a RBA platform called Smart Authentication to enhance the authentication services for stakeholders with the ultimate objectives of increasing transaction approvals, reducing fraud and improving the cardholder experience.

Mastercard provides a network-level authentication risk analysis of all Identity Check Transactions using EMV 3-D Secure that get processed through the DS. Mastercard as a network has the ability to see cardholder activity across the digital and physical worlds, and can use this expanded view to power its Smart Authentication platform.

In addition to cardholder authorization history and consistency of behavior, the Smart Authentication platform leverages cardholder authentication history and other unique data points provided by the EMV 3-D Secure data stream to provide a holistic assessment of the transaction's authentication risk.

A variety of Smart Authentication solutions will be introduced over time as Mastercard Identity Check gains scale with EMV 3-D Secure. Currently, Identity Check offers the following Smart Authentication services:

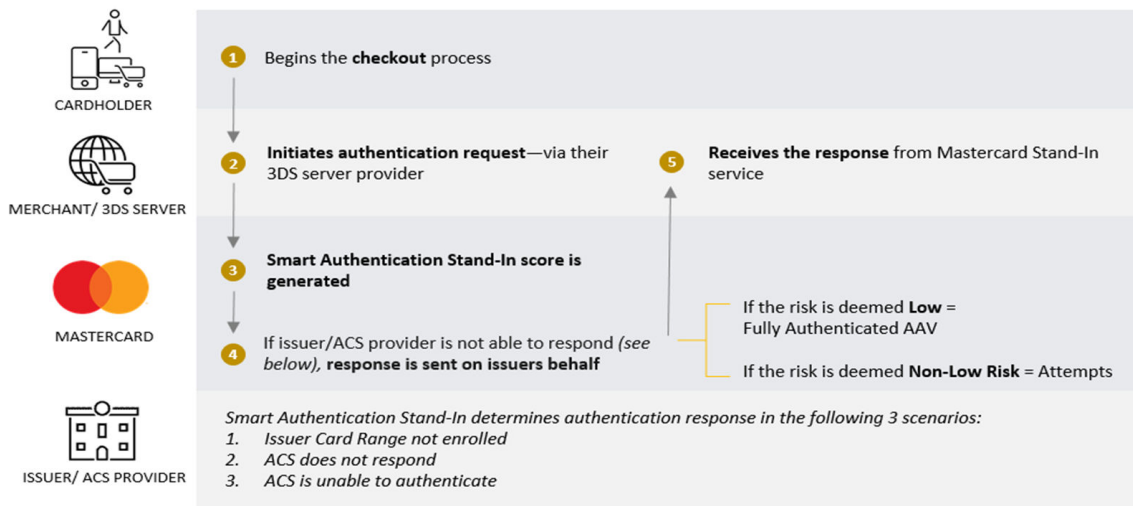
Smart Authentication Stand-In

The Smart Authentication Stand-In (previously known as Stand-In Risk-Based Authentication (RBA)) service is an on-behalf-of service provided for issuers by Mastercard to enable EMV 3-D Secure and facilitate a response to cardholder authentication requests on e-commerce transactions.

Smart Authentication Stand-in is required for issuers with certain exceptions. For more detail about Smart Authentication Stand-in, including exceptions, for regulated markets, refer to AN 1702, AN 2005, AN 2036, AN 2724, AN 2867. Smart Authentication Stand-In does not impact the liability shift of the transaction. The liability remains with the issuer, as with transactions that are authenticated by the issuers themselves. Smart Authentication Stand-In informs the issuer about the potential level of authentication risk based on analysis using the Mastercard Smart Authentication platform. The service identifies low risk EMV 3-D Secure transactions as fully authenticated on the issuer's behalf. If the service

identifies the transaction as non-low risk, a merchant only authentication (attempts) is generated.

Smart Authentication Stand-In helps ensure merchant authentication requests are always answered



Smart Authentication Stand-In will enable issuers in impacted markets that do not have an EMV 3-D Secure solution to respond to EMV 3-D Secure authentication requests from merchants.

Many markets, require issuers to authenticate their cardholders for many or all e-commerce transactions. When issuers respond to an authentication request, they generate fully authenticated transactions proving the cardholder is who they say they are. These fully authenticated transactions greatly enhance the cardholder’s shopping experience with increased trust, and lift approval.

When issuers do not respond to a merchant authentication request within a certain time frame or do not successfully authenticate the cardholder, they create more merchant-only authenticated transactions. These transactions signify uncertainty that the cardholder is who they say they are. These merchant-only authentications reduce trust across the ecosystem, leading to lower approval rates, higher occurrences of fraud and a poor cardholder shopping experience. Participation in EMV 3-D Secure, Identity Check, and Smart Authentication Stand-In extends the benefits of authentication to a broader set of e-commerce transactions across the globe.

This service applies to issuers receiving EMV 3-D Secure authentication requests when:

- The issuer is not participating in EMV 3-D Secure
- The card range is not enrolled with the issuer’s authentication solution
- The issuer’s authentication solution is unable to authenticate the cardholder because either

- The cardholder is not enrolled
- The issuer’s authentication solution is unavailable or not responding

The core benefits to the issuer include:

- Ability to participate in EMV 3-D Secure during the initial phases of roll out, and evaluate if the Smart Authentication Stand-In service is a viable long term solution.
- Additional security and protection on transactions when the issuer is liable for chargebacks.
- Address low approval rates and higher fraud rates on merchant-only transactions.

Issuer Readiness—issuers should update their authorization rules to differentiate between merchant-only and fully authenticated transactions, if they have not already done so.

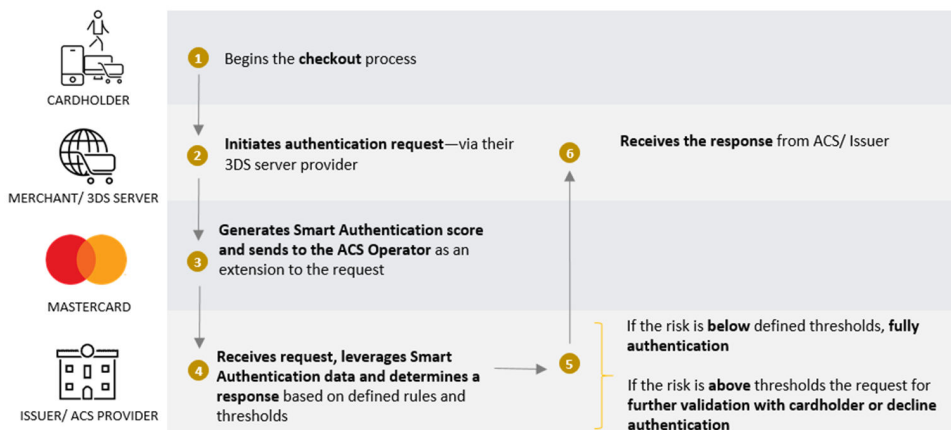
Smart Authentication for ACS/Issuers

Smart Authentication for ACS/Issuers (previously known as ACS RBA) is an optional service available to ACS and issuers, with certain exceptions.

Some ACS providers do not have any or only have rudimentary RBA capabilities. To bolster their overall authentication capabilities, and enable them to leverage the benefits of the EMV 3-D Secure protocol for their issuer’s customers, Mastercard supplies RBA intelligence for Mastercard transactions they process as a value added service. Once enrolled, Mastercard sends with the authentication risk assessment that the Mastercard Smart Authentication Platform generates for the transaction to the ACS as an extension to the Authentication Request (AReq) message within the EMV 3-D Secure protocol. The ACS can consume the intelligence as part of the authentication process.

Contact your Mastercard representative for additional information about Mastercard solutions for ACS providers. Refer to the *ACS RBA Supplemental Guide* in Mastercard Connect Publications for more information.

Smart Authentication for ACS/ Issuers can help issuers and ACS providers leverage data exchange offered by EMV 3-D Secure



Digital Transaction Insights (DTI)

Digital Transaction Insights (DTI), is a solution intended to help issuers fine-tune their authorization decisions with the goal of approving genuine transactions and declining fraudulent ones.

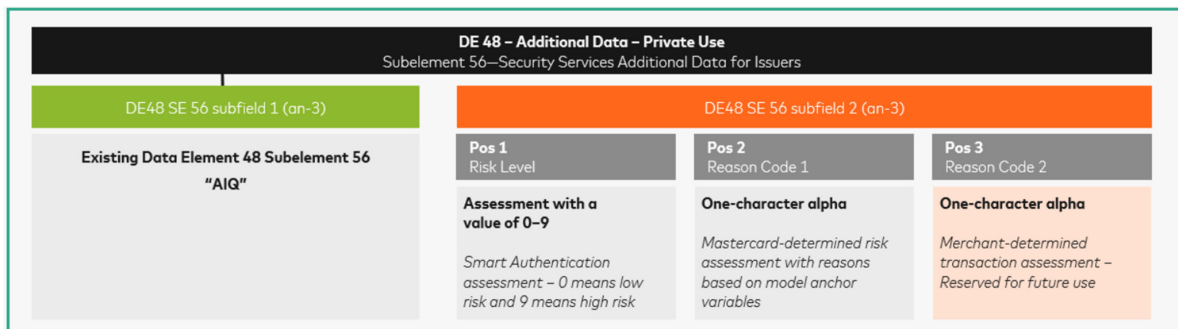
Recent enhancements in technology, artificial intelligence and the EMV 3-D Secure standardization have all enabled Mastercard to make advances to the Decision Intelligence product suite.

DTI is a service, previously known as Assurance IQ, that provides issuers with additional insights for card not present transactions.

DTI integrates the authentication and authorization platforms, facilitates a better customer experience and reduces the risk of fraud losses. DTI is designed to enable Mastercard to provide additional information about a transaction to help the issuer make an approval decision.

Merchants enable DTI to be shared with the issuer through the Mastercard Identity Check network whenever they submit an Identity Check transaction. The DTI will be published, where available, in the payment authorization message for all Identity Check transactions.

NOTE: In the future, Mastercard will also allow merchants to provide their assessment of the transaction as part of the DTI. This will allow the merchant and issuer to collaborate on transaction decisioning without additional friction or latency. This guide will be updated with further details in the future publications.



In order to minimize the processing impact, the DTI from the Smart Authentication platform are populated in Authorization in the former Assurance IQ fields - Data Element 48 (Additional Data - Private Use) Subelement 56 (Security Services Additional Data for Issuers). Subfield 1 are used as before to populate the "AIQ" key. The following information is shared in the Subfield 2

- Position 1 is Risk Level (Assessment with value 0-9 with 0 = low risk, 9 = high risk)
- Position 2 is Reason Code 1 (A to Z)—supports Mastercard-determined risk level assessment with reasons based on the Smart Authentication platform anchor variables

NOTE: The change from Assurance IQ is detailed in reason codes section.

- Position 3 is reserved for future use and will be used for Reason Code 2 (A to Z)— supports merchant-determined transaction assessment.

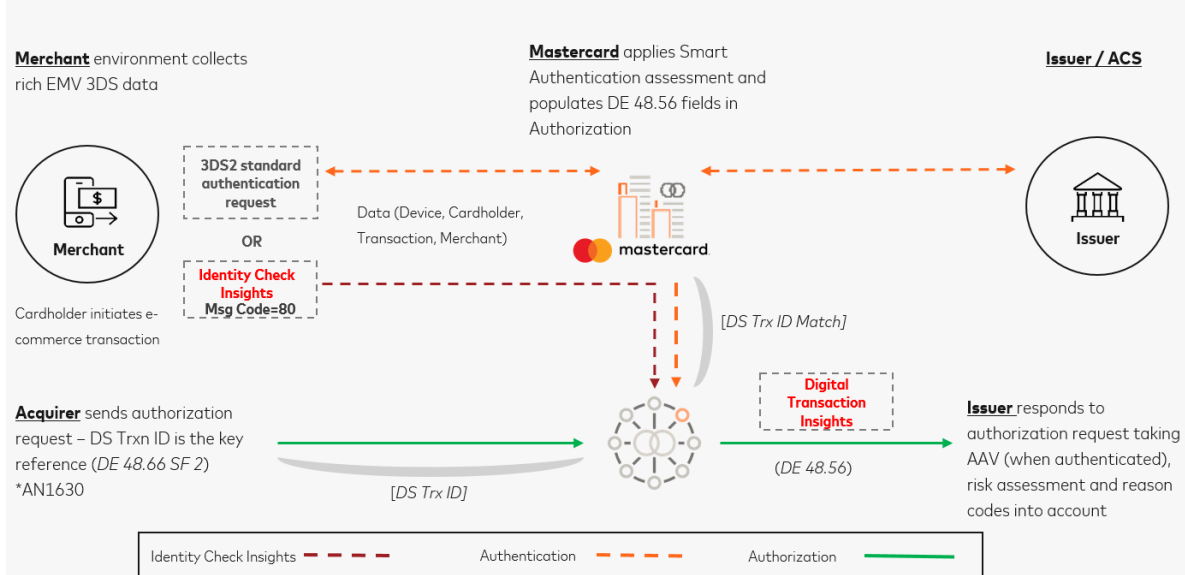
Even though the assessment (Risk Level) is the reference for issuer risk and fraud management decisioning (note the change from Assurance IQ assessment where nine (9) represented the greatest assurance or trust), it is the reason code that offers a more specific view on the driver of the Mastercard risk assessment. Values from A-Z represent these drivers, with A as highest risk to Z as most trusted reason. These data fields should supplement the issuer’s decision to authorize. See Appendix C *Digital Transaction Insights*, for details on Reason Codes.

As issuers and issuer processors have been required to receive the above data elements as part of the 2016 Global Safety and Security Roadmap and as communicated as part of the Assurance IQ and Decision Intelligence Global Operations Bulletins, there may not be additional development effort required to receive the fields for this service. If an issuer has already coded and tested DE48 Subelement 56 for another service (for example, Consumer Controls), the issuer does not need to go through additional coding, or testing with Mastercard.

Since the incremental risk analysis will be valuable to issuer risk and fraud management processes, or both, issuers and their processors may need to integrate the DTI presence and values into their processing. And if issuers were already consuming the insights, updates to the assessment and reason codes may require changes to how the insights are ultimately integrated and used.

The flow below offers an overview how Mastercard feeds DTI from authentication into authorization messages.

Bridging Authentication Insights into Authorization – How it Works



Message Types

There are different message types that are exchanged between the three domains of EMV® 3-D Secure in order to carry out authentication.

Those message types are:

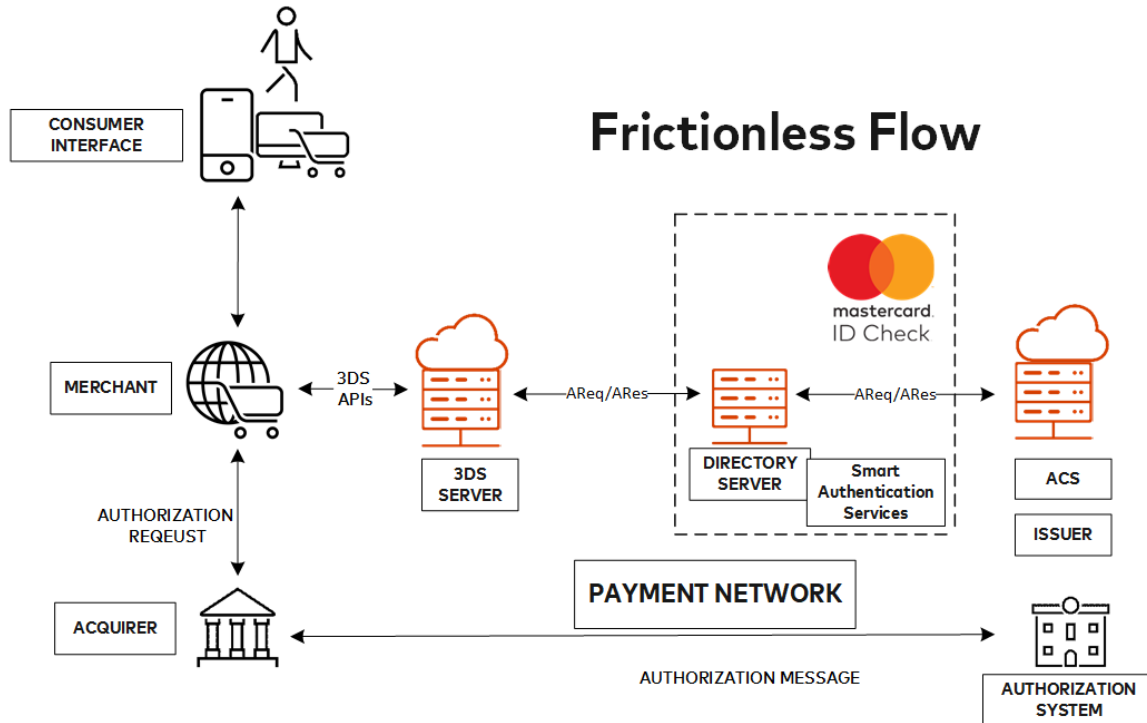
- Authentication Request (AReq) or Authentication Response (ARes): These are used in the frictionless and challenge authentication flows for exchanging authentication information between the 3-D Secure server and ACS through Mastercard Directory Server (DS).
- Challenge Request (CReq)/Challenge Response (CRes): These are only used in the Challenge/step-up flow when ACS/issuer requires more information from the cardholder in order to authenticate.
- Results Request (RReq)/Results Response (RRes): These are used to communicate the results of the authentication transaction after the challenge has been presented and completed in a transaction.
- Preparation Request (PReq)/Preparation Response (PRes): These are used for communication between the 3-D Secure Server and the DS when the 3-D Secure Server wants to gather information regarding the 3-D Secure protocol versions used by the ACS and DS, along with the 3-D Secure method URL.

NOTE: For more details on the message types, refer to *EMV 3-D Secure Core Specification*.

The [Liability Shift and Processing Matrix](#) section of this document provides details on the different authentication scenarios for the frictionless and challenge flows along with their corresponding transaction statuses across all the message types, ECI and AAV values, and expected values through the authorization and clearing processes.

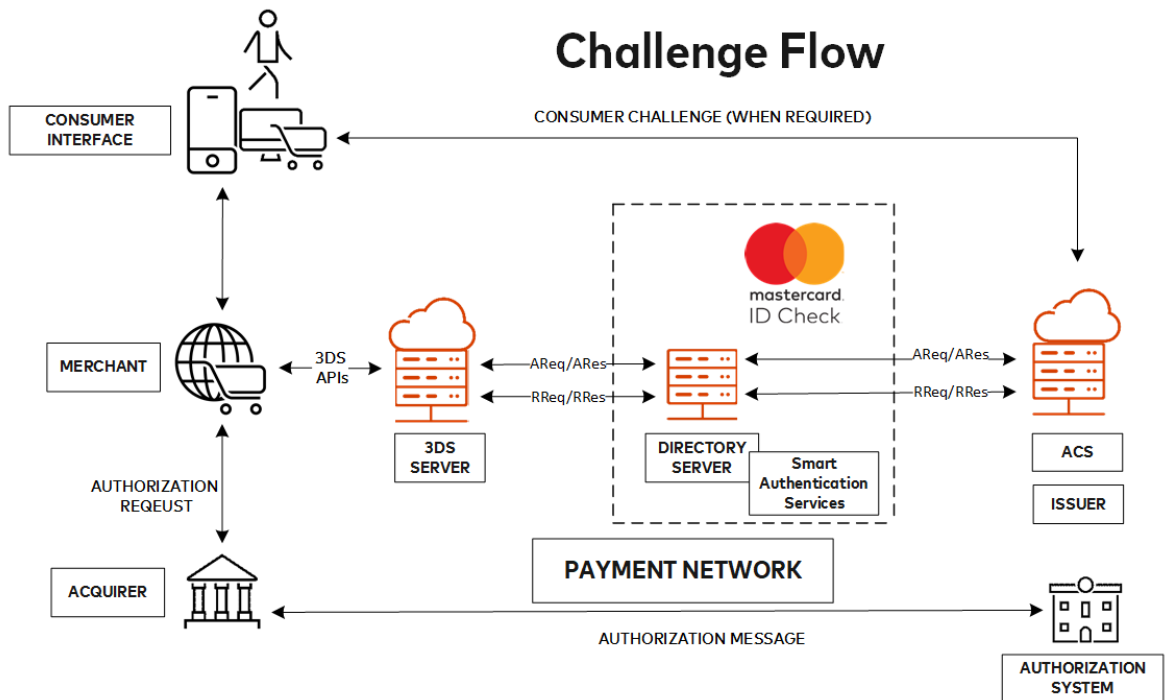
Mastercard Identity Check Use Cases

Mastercard Identity Check™ supports two primary use cases - the Frictionless flow and Challenge flow for payment authentication.



A Frictionless authentication flow demonstrates that the cardholder initiates the payment authentication, the transaction can be authenticated by way of risk-based decisioning, and no additional interaction is required.

- The 3-D Secure requestor sends an authentication message with all the necessary information required to formulate an AReq message to the 3-D Secure server.
- 3-D Secure server creates the AReq message and sends to Directory Server (DS).
- The DS adds risk scores and data needed to evaluate the risk of the transaction and sends to the Access Control Server (ACS)/issuer.
- ACS/issuer responds to DS with an ARes message indicating that no further interaction or information is required from the cardholder.
- The DS sends this message to 3-D Secure Server who in turn sends it to 3-D Secure requestor to complete the transaction with the cardholder.
- Merchant and issuer then work together to complete the business as usual authorization flow.



A Challenge/Step-up authentication flow demonstrates that the cardholder must perform additional steps such as entering a one-time pass code to successfully authenticate the transaction. Challenge flow is the same as a frictionless flow except that once the ACS issuer responds with the ARes message; it indicates that further interaction is required with the cardholder. This initiates a new set of messages, CReq and CRes between the 3-D Secure requestor and ACS/issuer where the challenge is performed. Then the ACS sends a RReq message to the 3-D Secure server through the DS, which responds with a RRes message to complete the transaction. Merchant and issuer then work together to complete the business as usual authorization flow.

Upon completion of a successful authentication through the Mastercard Identity Check program, a merchant realizes the full benefits of liability shift. For more information on processing and data requirements, refer to Chapter 4, [Liability Shift and Processing Matrix](#) of this document.

NOTE: For more details on the frictionless and Challenge flows, refer to *EMV 3-D Secure Core Specification*.

Additional Features

Mastercard offers several "features" beyond those normally supported by the EMV® 3DS specifications. This helps support certain use cases or needs for the stakeholders in the EMV 3DS ecosystem, not currently met by the specification.

Identity Check Insights

Identity Check Insights, previously referred to as "Data Only", is a Mastercard defined payment message category.

The Identity Check Insights message is an option that allows the merchant the flexibility to share data through the EMV® 3DS rails in order to generate authentication insights that could influence an issuer's decision to approve a transaction without requesting authentication. Thus, Identity Check Insights creates no risk of cardholder challenge and added latency. Just like payment authentication transactions, Digital Transaction Insights (DTI) are generated by Mastercard and sent to the issuer in Authorization to influence transaction decisioning.

NOTE: For more details on how DTI works, refer to *Digital Transaction Insights (DTI)* section of this document.

An Identity Check Insights message is identified by the value in the "Message Category" field defined by Mastercard. A normal authentication request is represented by message category 01 (payment) or 02 (non-payment), and Identity Check Insights (without authentication) is requested using Mastercard message category value of 80.

NOTE: Regardless if the merchant has requested authentication or is sending Identity Check Insights, Mastercard will run all EMV 3DS transactions through the Mastercard Smart Authentication (RBA) engine and generate DTI.

Identity Check Insights Process and Technical Readiness

In an Identity Check Insights transaction message, because the issuer is not receiving an authentication request, there is no fraud liability shift to the issuer.

The steps below describe how an Identity Check Insights message is created, the responsibilities of the parties in the ecosystem for successful creation and the associated response.

1. Merchant can submit an EMV® 3DS request for "Identity Check Insights" indicating
 - a. Message Category = 80 – Mastercard message
 - b. Device channel – 01 App or 02 BRW (3RI Device Channel is not currently supported)
2. 3D Secure Server must validate the request based on message category 80, with Mastercard BIN and device channel combination and then create the AReq.
 - a. Message Category 80 – must be validated by the 3D Secure Server using the same rules as a 01-payment request. Data elements in the request must include all required fields for an AReq with Message Category of 01-PA request as defined by

- EMV. If a request is submitted with missing required fields, then the 3D Secure Server must stop processing and submit an error to the requestor.
- b. If a request is submitted with 3RI as a device channel, then the 3D Secure Server must stop processing and submit an error to the requestor.
 - c. The 3D Secure server then must route requests with Message Category 80 to the Mastercard Directory Server (DS) by creating an EMV compliant AReq message.
3. Mastercard Directory Server (DS) validates the Identity Check Insights message and then forwards it to the Mastercard Smart Authentication platform.
- a. Once the Mastercard Smart Authentication platform processes the message, an ARes message is provided back by the DS to 3D Secure server with a unique DS transaction Id for that transaction. For a sample response, refer to Appendix I - Identity Check Insights - Sample Responses.
 - b. If the message was not successfully processed, then the failure is communicated to the 3D Secure Server by using the “maiqRes” message extension.

NOTE: For an example of failure response using the “maiqRes” message extension, refer to Appendix I - Identity Check Insights - Sample Responses.

4. The 3D Secure server must then validate received ARes and transform it into a response, and be provided back to the requestor merchant.
5. Requestor must leverage the DS Transaction ID provided in the response, to submit in the Authorization message. The details of the Smart Authentication assessment are provided to the issuer in the Authorization flow as DTI.
Refer to associated program requirements in "Mastercard Identity Check Transaction Processing Requirements" section of Chapter 4 of this guide.

For an illustration of how the Identity Check Insights transaction works, refer to Appendix N - Mastercard Identity Check Insights Transaction Flow.

Acquirer Strong Consumer Authentication (SCA) Exemption

EMV[®] 3DS version 2.2 has additional values added to the 3DS Requestor Challenge Indicator field to allow for improved communication between merchants and issuers for the purposes of exemptions for Strong Consumer Authentication (SCA) to be applied.

Mastercard Identity Check not only supports these new values for version 2.2 but also offers the same capability in version 2.1 by defining a Mastercard specific Message Extension. This additional feature helps maximize the benefit of the available exemptions.

NOTE: For requirements on acquirer SCA exemptions for EUR, refer to the “acquirer SCA exemptions” section of Chapter 5.

The table below details how Acquirer SCA Exemption can be requested for the different versions of the EMV 3DS.

NOTE: For version 2.1, a successful exemption request will result in a transaction status = N with reason code 81, along with the presence of an AAV with a leading indicator kN and an ECI=06. 3DS Servers and merchants must ensure that they ALWAYS look at the reason code along with Status of N to make sure they do not falsely end up rejecting a successful exemption transaction.

Table 1: Feature: Acquirer SCA Exemption

3DS Version	Network	Description	
		Data Element	Values
2.1	Authentication	Message Flow	AReq = O
		Message Category	01- PA and 02- NPA
		Device Channel	01- App, 02- Browser, and 03-3RI
		Request Message	
		“Merchant Data” Message Extension field “scaExemptions”	05 = No challenge requested (transactional risk analysis is already performed).
		3DS Requestor Challenge Indicator	02 = (No challenge requested)
		<p>NOTE: The value of 05 in the scaExemptions field is used to indicate SCA exemption request for all four types of possible SCA exemptions – namely Merchant Initiated Transaction, Acquirer low fraud and Transaction Risk Analysis, Recurring payment and Low value payments.</p>	
<p>NOTE: For details on Merchant Data Message Extension refer to Appendix D - Merchant Data Message Extension.</p>			
Response Message (ARes)			
	Transaction Status	N	
	Transaction Status Reason	81 = “challenge exemption accepted”	
	ECI	06	
	AAV leading Indicator	kN	
<p>NOTE: Response to a un-authenticated SCA exemption request will be BAU.</p>			

3DS Version	Network	Description					
		Data Element	Values				
		<p>NOTE: For details around transaction processing refer to the Processing Matrix in Chapter 4.</p> <hr/> <p>NOTE: For the Payment Transaction Message Flow for version 2.1, refer to Appendix F - Payment Transaction Flow (version 2.1 and 2.2).</p>					
	Authorization	<p>Successfully authenticated Acquirer SCA exemption transactions are submitted in Authorization with the below.</p> <hr/> <table border="1"> <tr> <td>SLI</td> <td>216</td> </tr> </table> <hr/> <table border="1"> <tr> <td>Data Element 48, sub-element 22, subfield 1 (DE48 SE22 SF1)*</td> <td> <p>One of the following</p> <ul style="list-style-type: none"> • 01 = Merchant Initiated Transaction • 02 = Acquirer low fraud and Transaction Risk Analysis • 03 = Recurring payment • 04 = Low value payment </td> </tr> </table> <hr/> <p>* DE48, SE 22, SF1 is optional globally but is required for Europe.</p> <hr/> <p>NOTE: Liability for this transaction is with the Acquirer.</p> <hr/> <p>NOTE: For a mapping of transaction status with AAV leading indicator, ECI, SLI and Liability, refer to Appendix L - Transaction Status, SLI , and Liability Mapping.</p>		SLI	216	Data Element 48, sub-element 22, subfield 1 (DE48 SE22 SF1)*	<p>One of the following</p> <ul style="list-style-type: none"> • 01 = Merchant Initiated Transaction • 02 = Acquirer low fraud and Transaction Risk Analysis • 03 = Recurring payment • 04 = Low value payment
SLI	216						
Data Element 48, sub-element 22, subfield 1 (DE48 SE22 SF1)*	<p>One of the following</p> <ul style="list-style-type: none"> • 01 = Merchant Initiated Transaction • 02 = Acquirer low fraud and Transaction Risk Analysis • 03 = Recurring payment • 04 = Low value payment 						

Table 2: Feature: Acquirer SCA Exemption

3DS Version	Network	Description	
		Data Element	Values
2.2	Authentication	Message Flow	AReq = O
		Message Category	01- PA and 02- NPA
		Device Channel	01- App, 02- Browser, and 03-3RI

3DS Version	Network	Description	
		Data Element	Values
		Request Message	
		3DS Requestor Challenge Indicator	05 = No challenge requested (transactional risk analysis is already performed).
		Response Message (ARes or RReq)	
		Transaction Status	I
		ECI	06
		AAV leading Indicator	kN
		<p>NOTE: If DS receives an ECI=06, it will validate if 3DS Requestor Challenge Indicator= 05 or not. If not, an error will be sent to the ACS</p>	
		<p>NOTE: Response to a un-authenticated SCA exemption request will be BAU.</p>	
		<p>NOTE: For details around transaction processing refer to the Processing Matrix in Chapter 4.</p>	
		<p>NOTE: For the Payment Transaction Message Flow for version 2, refer to Appendix F - Payment Transaction flow (Version 2.1 and 2.2).</p>	
	Authorization	<p>Successfully authenticated Acquirer SCA exemption transactions are submitted in Authorization with the below.</p>	
		SLI	216
		Data Element 48, sub-element 22, subfield 1 (DE48 SE22 SF1)*	<p>One of the following</p> <ul style="list-style-type: none"> • 01=Merchant Initiated Transaction • 02=Acquirer low fraud and Transaction Risk Analysis • 03=Recurring payment • 04=Low value payment
		<p>* DE48, SE 22, SF1 is optional globally but is required for Europe.</p>	

3DS Version	Network	Description	
		Data Element	Values
NOTE: Liability for this transaction is with the Acquirer.			
NOTE: For a mapping of transaction status with AAV leading indicator, ECI, SLI and Liability, refer to Appendix L - Transaction Status, SLI , and Liability Mapping.			

Acquirer SCA Exemptions can also be requested directly in an authorization transaction (no authentication) with SLI = 210 (not Authenticated) using the same values in Data Element 48, sub-element 22, subfield 1 (DE48 SE22 SF1) as indicated in the table above.

Merchant Fraud Rate

Mastercard allows merchant fraud rate to be shared with the ACS/Issuer as part of the AReq message using a Mastercard specific Message Extension.

Sharing the merchant fraud rate can increase the ACS/Issuer’s level of confidence in the transaction. Issuers may also use it to decide if a merchant should be eligible for the white listing exemption.

NOTE: Some regulated countries may have guidance on how fraud rates must be calculated. For requirements on fraud rate calculations for EUR, refer to the “Merchant Fraud Rate” section of Chapter 5.

The table below details how merchant fraud rate can be shared.

NOTE: This works the same way for version 2.1 and 2.2 of EMV 3DS.

Table 3: Feature: Merchant Fraud Rate

3DS Version	Network	Description	
		Data Element	Values
2.1 & 2.2	Authentication	Message Flow	AReq = O
		Message Category	01- PA
		Device Channel	01- App, 02- Browser, and 3RI
		Request Message	

3DS Version	Network	Description	
		Data Element	Values
		“Merchant Data” Message Extension field “merchantFraudRate”	1 (represents fraud rate <=1) 2 (represents fraud rate 1+ - 6) 3 (represents fraud rate 6+ - 13) 4 (represents fraud rate 13+ - 25) 5 (represents fraud rate >25)
		<p>NOTE: For details on Merchant Data Message Extension, refer to Appendix D - Merchant Data Message Extension.</p> <hr/> <p>Response Message (ARes or RReq)</p> <p>The response messages will follow BAU processing logic.</p>	
	Authorization	The authorization messages will follow BAU logic based on the result of the authentication message.	

Acquirer Country Code

The merchant country and the acquirer country for transactions may be different.

Issuers may need to be aware of the acquirer country code, especially when it differs from the merchant country. This becomes particularly important for some regulated countries where regulations may apply based on the acquirer country.

NOTE: For requirements on acquirer country code for EUR, refer to the “acquirer country code” section of Chapter 5.

Mastercard allows for sharing of acquirer country code using Mastercard defined message extension. The table below details how the acquirer country code can be shared.

NOTE: This works the same way for version 2.1 and 2.2 of EMV 3DS.

Table 4: Feature: Acquirer Country Code

3DS Version	Network	Description	
		Data Element	Values
2.1 & 2.2	Authentication	Message Flow	AReq = O
		Message Category	01- PA and 02- NPA
		Device Channel	01- App, 02- Browser, and 3RI
		Request Message	
		"Merchant Data" Message Extension field "acquirerCountryCode"	Any numeric ISO country code
		NOTE: For details on Merchant Data Message Extension refer to Appendix D - Merchant Data Message Extension.	
Response Message (ARes or RReq)			
		The response messages will follow BAU processing logic.	
Authorization		The authorization messages will follow BAU logic based on the result of the authentication message.	

NOTE: Mastercard will recognize non-ISO country codes as valid if the country code is supported on the GCMS production tables found in the Quick Reference Booklet Chapter 2. For example, The Republic of Kosovo does not have an ISO country code defined. Mastercard has defined a code for Kosovo, United Nations Mission in Kosovo (UNMIK) in Authorization and Clearing (numeric country code = 900), and Netherlands Antilles (numeric country code = 530). In order to make sure that authentications from that country code are recognized, ACSs must synchronize their country code list with the ISO country code list and Mastercard GCMS production tables.

NOTE: The Mastercard Member Parameter Extract (MPE) table maps the Issuer country related to a BIN as well as the Acquirer country to the acquirer's Mastercard Customer ID. Merchants can receive an extract of the MPE tables from their acquirers or can obtain the BIN table, called the "BIN Table Resource" from Mastercard. For more information on the BIN Table Resource, refer to Appendix H - BIN Table Resource.

Merchant Whitelisting

Merchants can be whitelisted by a cardholder therefore choosing to bypass SCA (Strong Customer Authentication) whenever they make a purchase from that Merchant.

ACS can indicate which card ranges are eligible for whitelisting while enrolling card ranges using the ISSM tool into the Mastercard DS. This data will then be reflected on the PRes

message through the 'ACS Information Indicator field' as part of version 2.2. Version 2.1 of the specification does not support this field, and therefore, this information will not appear on the PRes.

In this process an ACS enables the cardholder to place the 3DS Requestor on their trusted beneficiaries list. Only the ACS and Cardholder can initiate Whitelisting as part either of an authentication transaction or separately. The DS does not maintain cardholder Whitelist status.

Recommendation: ACS/Issuers must obtain from the cardholder an express informed consent; it should be clear to him or her what he or she is agreeing to, including which entity, or entities, was white listed and in which countries and for which products and services (in case an entity provides multiple products and services). This can be achieved by adding a link to the terms and conditions.

NOTE: This requirement is similar to setting up a direct debit (that is, e-mandate).

Recommendation: ACS/Issuers must allow cardholders to opt-out of Whitelisting services altogether and must also allow cardholders to view, add and remove, or both, merchants from their white list.

NOTE: For recommended best practices on cardholder user experience for adding merchants and for managing the merchant white list, risk considerations and operational considerations, refer to the *Mastercard Standards for Merchant White Listing*.

Whitelisting Request during Authentication Transaction

Version 2.2 of the specification allows merchants to request whitelisting as part of the authentication transaction. Below are details on how that works.

NOTE: This feature is supported only for version 2.2 of the specification and is not applicable to 3RI or Identity Check Insights transactions. Smart Authentication Stand-in cannot be applied to whitelisting requests.

Table 5: Feature: Merchant Whitelisting During Authentication Transaction

3DS Version	Network	Description	
		Data Element	Values
2.2	Authentication	Message Flow	AReq = O
		Message Category	01- PA and 02- NPA
		Device Channel	01- App, 02 - Browser
		Request Message	
		3DS Requestor Challenge Indicator	09 = Challenge requested (whitelist prompt requested if challenge required)

3DS Version	Network	Description	
		Data Element	Values
Response Message (ARes or RReq)			
		Transaction Status	BAU processing applies. The Whitelist status must not impact the status of the transaction.
		Whitelist Status	<ul style="list-style-type: none"> • Y = 3DS Requestor is whitelisted by cardholder • N = 3DS Requestor is not whitelisted by cardholder • R = Cardholder rejected (not supported in Areq) • E = Not eligible as determined by issuer (not supported in Areq) • P = Pending confirmation by cardholder (not supported in Areq) • U = Whitelist status unknown, unavailable, or does not apply (not supported in Areq)
		Whitelist Status Source	03 = ACS
NOTE: Whitelist status can still be a "Y" for an un-authenticated transaction.			
Authorization		The authorization messages will follow BAU logic based on the result of the authentication message.	

Whitelisting Status Response

While the version 2.2 of the specification allows ACS to share the status of whitelisting using the "whitelist Status" field like mentioned earlier in this document, version 2.1 of the specification does not support this field.

Mastercard Identity Check offers the capability for ACS to share the whitelist status with the requestor or merchant in version 2.1 by defining a Mastercard specific Message Extension. The table below details how the whitelist status can be shared.

NOTE: This is applicable to version 2.1 of EMV® 3DS.

Table 6: Feature: Whitelist Status Response for Version 2.1

3DS Version	Network	Description	
		Data Element	Values
2.1	Authentication	Message Flow	ARes = O
		Message Category	01- PA and 02- NPA
		Device Channel	01- App, 02- Browser, and 3RI
		Request Message	
		The request message will follow BAU processing logic. Whitelisting cannot be requested by the merchant in version 2.1.	
		Response Message	
		“ACS Data” Message Extension field “whitelistStatus”	<ul style="list-style-type: none"> • Y = 3DS Requestor is whitelisted by cardholder • N = 3DS Requestor is not whitelisted by cardholder • E = Not eligible as determined by issuer • P = Pending confirmation by cardholder • R = Cardholder Rejected • U = Whitelist status unknown, unavailable, or does not apply
		<p>NOTE: If the “ACS Data” Message Extension “whitelistStatus” field is passed in version 2.2, then DS will drop the field and continue processing. For details on ACS Data Message Extension, refer to Appendix E - ACS Data Message Extension.</p>	
		<p>NOTE: The response messages will follow BAU processing logic if the “ACS Data” Message Extension “whitelistStatus” field is passed in version 2.2, then DS will drop the field and continue processing.</p>	
		Authorization	The authorization messages will follow BAU logic based on the result of the authentication message.

Whitelist Exemption

Once the merchant gets successfully whitelisted (whitelist Status = Y), then they can use the whitelist exemption in subsequent transactions.

The table below details how the subsequent transactions from that merchant can use the whitelisting exemption.

NOTE: This is only applicable to version 2.2 of the EMV 3DS.

Table 7: Feature: Whitelist Exemption

3DS Version	Network	Description	
		Data Element	Values
2.2	Authentication	Message Flow	AReq = O
		Message Category	01- PA and 02- NPA
		Device Channel	01- App, 02 - Browser
		Request Message	
		Whitelist Status	Y = 3DS Requestor is whitelisted by cardholder
		Whitelist Status Source	01 = 3DS Server
		3DS Requestor Challenge Indicator	08 = No challenge requested (utilize whitelist exemption if no challenge required)
		Response Message (ARes)	
		Whitelist Status	Y = 3DS Requestor is whitelisted by cardholder
		Whitelist Status Source	03 = ACS
		Transaction Status	Y
		ECI	02
		AAV leading Indicator	kA
		NOTE: Response to a unauthenticated whitelist exemption request will be BAU.	
NOTE: For details around transaction processing, refer to the Processing Matrix in Chapter 4.			
	Authorization	Successfully authenticated Whitelist exemption transactions are submitted in Authorization with	

3DS Version	Network	Description	
		Data Element	Values
		SLI	212

NOTE: Liability for this transaction is with the issuer.

Whitelist Status Check

A merchant can check the status of their whitelisting using 3RI payment or non-payment transaction in version 2.2 of EMV 3DS. The table below details how this works.

Table 8: Feature: Whitelist Status Check

3DS Version	Network	Description	
		Data Element	Values
2.2	Authentication	Message Flow	AReq = R
		Message Category	01- PA and 02- NPA
		Device Channel	03 - 3RI
		Request Message	
		Whitelist Status	Y = 3DS Requestor is whitelisted by cardholder
		Whitelist Status Source	01 = 3DS Server
		3RI Indicator	10 = Whitelist status check
Response Message (ARes)			

3DS Version	Network	Description	
		Data Element	Values
		Whitelist Status	<ul style="list-style-type: none"> • Y = 3DS Requestor is whitelisted by cardholder • N = 3DS Requestor is not whitelisted by cardholder • E = Not eligible as determined by issuer • P = Pending confirmation by cardholder • R = Cardholder Rejected • U = Whitelist status unknown, unavailable, or does not apply
		Whitelist Status Source	03 = ACS
		NOTE: The response messages will follow BAU processing logic.	
	Authorization	The authorization messages will follow BAU logic based on the result of the authentication message.	

AAV Refresh

Mastercard generates an Account holder Authentication Values (AAV) for every successfully authenticated payment transaction. Mastercard retention and validity period for an AAV is 10-90 days.

For certain payment scenarios like recurring payments, the time lapse between authentication and authorization might be more than the AAV's retention period. In that case, the payment transaction will have to be submitted in authorization without an AAV (SLI = 210) even though the transaction was initially authenticated.

To solve for this, Identity Check offers the “AAV Refresh” capability. This capability allows merchants to request a ‘refreshed’ AAV (using a non-payment (NPA) AReq) from the issuer ACS for their previously fully authenticated transaction. The ACS then analyzes the request and shall determine if the AAV must be refreshed or not. If refreshed, an ARes is returned to the merchant containing the new refreshed AAV with new leading indicator of kQ, ECI=N2 (authenticated), and Transaction Status = Y.

The merchant can then submit the corresponding authorization as a fully authenticated transaction (SLI= 212) and continue to benefit from liability shift even if the time lapse between the original authentication and authorization is more than 90 days.

NOTE: For more information on SLI, ECI, and Leading Indicator mapping, refer to Appendix L.

Below are some program requirements associated with an AAV Refresh:

Requirement 135: A Merchant shall only request an 'AAV Refresh' after the current AAV is expired.

Requirement 136: An 'AAV Refresh' request shall only be requested by the merchant using Device Channel = 3RI ("03"), Message Category = NPA ("02"), and 3RI Indicator = ("81") of the Authentication Request (AReq) for version 2.1 of EMV® 3DS.

NOTE: AAV refresh capability is not supported for version 2.2 of EMV 3DS as 3RI payments (PA) can be used to generate a new AAV if the AAV's validity period is past.

Requirement 137: An 'AAV Refresh' 3RI Non-Payment transaction's 3DS Requestor Prior Transaction Authentication Data (Field Name: threeDSReqPriorAuthData) field must be used to reference the DS transaction ID of the initial authentication transaction (frictionless or challenge) the AAV refresh is tied to.

Requirement 138: An 'AAV Refresh' 3RI Non-Payment transaction's Purchase Amount (Field Name: purchaseAmount) field must indicate the amount for which the new refreshed AAV is requested.

Requirement 139: ACS shall respond with a Transaction Status = Y, an ECI = N2 (Authenticated) and an IAV if the AAV Refresh request was successful. They shall not challenge or step-up an AAV request message.

NOTE: Mastercard Smart Authentication Stand-in service does not apply to an AAV refresh request. Thus, Mastercard will not stand-in on behalf of an issuer ACS and generate a refreshed AAV if the issuer ACS is not available.

NOTE: This is currently the only Identity Check use case where an AAV is generated for a non-payment (NPA) transaction.

Mastercard On-behalf AAV Validation Service

During authentication, a unique DS Transaction ID is generated by Mastercard and provided to both issuer's ACS and the merchant.

The issuer's ACS generates an IAV, a cryptogram, to confirm that the authentication was approved. Mastercard generates the remaining part of the Cryptogram to form the full SPA2 AAV.

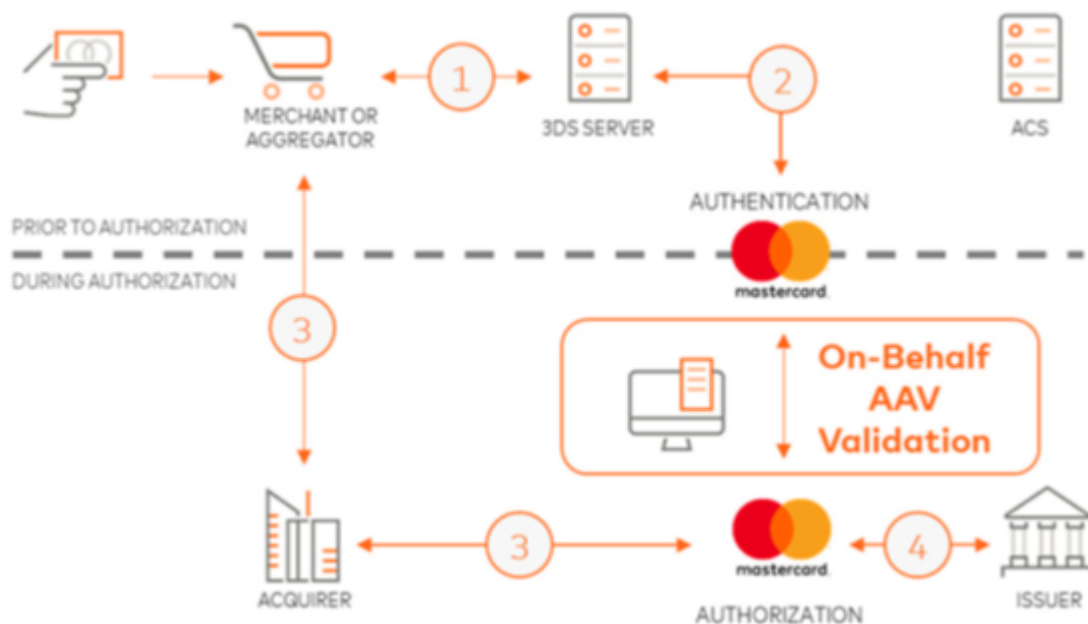
The merchant provides the DS Transaction ID along with the AAV in the authorization message. AAV validation takes place in authorization. This can be done by the issuers themselves by performing 'self-validation', or can be done by Mastercard on behalf of the issuer using the Mastercard On-Behalf of Services (OBS).

The Mastercard retention period for an AAV is 10-90 days.

Requirement 146: Issuers must retain and must be able to validate AAVs for at least 90 days if self-validating.

Self-validation by issuers poses some challenges like complexity of the IAV validation and the requirement to exchange keys with their ACS.

Mastercard is ideally placed to provide on-behalf AAV validation service as this service does not require any key exchange. The Mastercard authentication and authorization networks are residing on connected platforms allowing easy and fast enhanced AAV Verification which verifies the PAN, SPA2 AAV, DS Transaction ID and amount between authorization and authentication. References the SPA2 AAV Guide for Mastercard Identity Check found on Mastercard Publications.



If the DS Transaction ID (despite a program requirement to provide it) is not provided, then the on-behalf AAV validation will verify the authentication with the authorization based on the AAV and card number.

For more information on how issuers can enroll into the Mastercard on-behalf AAV validation service, refer to the SPA2 AAV Guide for Mastercard Identity Check on Mastercard Publications.

Chapter 3 Mastercard Identity Check Global Program Requirements

This section describes the requirements for the Mastercard Identity Check™ Program that ensures a smooth consumer authentication experience.

Mastercard Identity Check Engagement Requirements.....	54
Approved Methods for Authentication.....	56
Authentication Methods Not Allowed.....	59
Authentication Experience Requirements.....	60
User Interface Requirements for App-based Transaction Flows.....	61
Key Performance Indicators—Compliance Measures.....	62
Privacy and Data Protection Matters.....	64
Requirements for Authentication Method.....	72
Risk Based Authentication.....	73
Biometric Authentication.....	74
Biometric—Fingerprint Match.....	74
Biometric—Facial Recognition.....	75
Biometric—Voice Recognition.....	75
Interactive Cards with PIN Pads.....	76
Push Notification Requesting Transaction Approval.....	76
Hand-held Token Generators/Fobs.....	77
One-Time Passcode through SMS.....	78
One-Time Passcode through Mobile App.....	78
Issuer Portal Verification.....	79
Fallback Method Using Email.....	79
Payment Transactions.....	81
Regular e-Commerce Payment Transaction	81
3RI Payments	81
Delayed Delivery/Charged.....	82
Partial Split Shipment	82
Payment Initiated by a Different Merchant.....	83
Agent Payment (with Multiple Merchants)	83
Unknown and Undefined Final Amount before Purchase.....	84
Installment Payments.....	85
Refund of a Purchase	86
Replacement (Re-authorization) of a Refunded Purchase	86

Adding Card-on-File—Regular Payment.....	87
Adding Card-on-File—Recurring Payment.....	87
Mail Order / Telephone Order (MOTO).....	88
Recurring Payments.....	88
Recurring Payment with Fixed Amounts	92
Recurring Payment with Variable Amounts	92
Recurring Payment Combined with One-time Purchase.....	93
Recurring Payment with Fixed Limit and Threshold	94
Use of Account Status Inquiry (ASI) in Recurring Payment.....	94
Non-Payment Transactions.....	95

Mastercard Identity Check Engagement Requirements

The Mastercard Identity Check™ program requires contact information and adherence to acceptable cardholder communication methods as well as compliance that are identified here.

Identity Check Program requires Program Participants to

Requirement 1: Adhere to the on-boarding rules and requirements laid out in the Identity Check on-boarding guides. Refer to the *Related Documentation* section.

Requirement 2: Adhere to all rules and requirements set forth in the EMV®Co 3-D Secure Specifications. Refer to the *Related Documentation* section.

Requirement 3: All Program Participants are required to keep their contact information up to date in the Mastercard Customer Contact Management (CCM) tool called "My Company Manager", (new generation of the *Mastercard Member Information Manual (MIM)*).

Program Registrant Contact Information

The Mastercard customer contact management tool "My Company Manager" is used to list various contacts within an institution for servicing products and applications.

The contact name listed in My Company Manager should be familiar with the Identity Check™ authentication program and solution implemented.

To access the My Company Manager application on Mastercard Connect™ go to:
Mastercard Connect > Store > Applications > My Company Manager > Contact (Contact Type: Mastercard Identity Check).

Acceptable Cardholder Communications

Requirement 4: Issuers must educate their cardholders about Identity Check and the authentication experience.

This includes

- Notifying cardholders before and after enrollment.
- Notifying cardholders when the issuer changes the authentication experience (such as, when changing from static password to a Mastercard Identity Check risk-based authentication approach).

Cardholders may be notified using any of the following methods

- Direct mail or post-mailer (either at the time of card delivery or through a separate communication)
- Phone (at the time of card activation)
- Email message
- Within the online bank site
- Within a mobile application

Cardholder Communications and Enrollment—Not Supported

Identity Check will promote shopping experiences with the least amount of friction required and will not support any form of cardholder recruitment during the checkout or purchasing journey.

Within the Identity Check program, the following cardholder communication methods will not be supported

- Activation during shopping
- ID&V process during shopping
- Requirement to call the issuer call center for the ID&V during shopping

Authentication Processing Requirements

Identity check program has some minimum requirements for issuers enrolling their card ranges into the program as highlighted below:

Requirement 141: All issuer account ranges must support challenge and frictionless transactions.

Requirement 142: All issuer account ranges must support in-app and browser transactions.

Requirement 152: All issuer account ranges must support payment and non-payment transactions.

Software Vendor Service Provider-Compliance

Requirement 5: Mastercard requires all ACS and 3-D Secure Server Providers to maintain compliance with the Mastercard ACS Compliance program or the Mastercard 3DSS Compliance Program, whichever is applicable. For the compliance program guides, refer to *Related Documentation* section.

The Mastercard compliance program ensures EMVCo and Mastercard program testing has been completed, all Mastercard program Key Performance Indicators (KPIs) are being met, and all 3-D Secure software has gone through the appropriate security assessments (PCI 3-D Secure).

Navigate to URL: www.mastercard.us/en-us/merchants/safety-security/securecode/securecode-vendors.html to reference the approved authentication vendors and their compliance status.

Requirement 87: If card account ranges are being enrolled onto the Mastercard DS for authentication routing, then the Identity Check Program logo must be displayed regardless if it is a Private Label (PVL) card.

Requirement 143: Test data or test transactions are not allowed in the Production environment. Mastercard reserves the right to remove Operator IDs or MIDs if high error rates are seen in Production. For language on bad data or test data, refer to the Identity Check T&Cs.

Approved Methods for Authentication

The table below lists the permitted authentication methods for primary and fallback authentication methods with the Mastercard Identity Check™ Program.

The solutions listed under primary are the first method used to authenticate the cardholder. The solutions listed under fallback will be used when the primary method is unavailable.

Requirement 6: Issuers should evaluate their authentication practices to ensure that they comply with the methods outlined below.

Requirement 88: Strong Customer Authentication (SCA) shall be designed to offer an ideal consumer experience while optimally securing payments.

NOTE: For additional details about each of the allowed authentication methods, refer to *Requirements for Authentication Methods* section of this document. For more information on Strong Consumer Authentication, refer to *Appendix A, Mastercard Authentication Best Practices* of this document.

Authentication Method Type	Description
Primary	<p>The primary methods highlighted in bold below are the Identity Check methods that offer positive consumer experiences at checkout:</p> <ul style="list-style-type: none"> • Frictionless Authentication through Risk Based Authentication (RBA) • Challenge Authentication with one of the following approved challenge methods: <ul style="list-style-type: none"> – Dynamic One-time Passcode (by way of SMS, push notification, or mobile app) – Biometric Fingerprint Match – Biometric Facial Recognition – Biometric Voice Recognition (when combined with device data and another factor such as dynamic code) – ChipTAN - Chip Transaction Authentication Number (TAN) as a form of single use one-time password – PhotoTAN - Photo Transaction Authentication Number (TAN) like QR Code as a form of single use one-time password – Interactive Cards with PIN Pads – Push notification requesting transaction approval from Cardholder (out of band method). – Hand-held Token Generators, such as key fobs (when method is shared with online banking). – Issuer Portal Verification Method, which requires the cardholder to log into the issuer site for verification.

NOTE: The issuer is responsible for ensuring that the fraud levels and declines are within the guidelines.

Authentication Method Type	Description
Fallback	<p>The fallback methods listed below are highly recommended for use when the primary authentication method is not available or fails due to technical reasons:</p> <ul style="list-style-type: none">• Email with one-time use passcode• SMS or push notification with one-time use passcode <p>NOTE: The fallback method is not intended to be a secondary method of authentication (for example, when the cardholder has failed the primary authentication method).</p>

Authentication Methods Not Allowed

The table below identifies the authentication methods that are not allowed because over time, these methods have proven burdensome to cardholders and much less effective in combating fraud.

Authentication Method Type	Description
Not allowed for Primary or Fallback Authentication	<ul style="list-style-type: none"> • Static passwords including random static passwords • Bingo or Transaction Authentication Number (TAN) cards • Static PIN entry into browser in online environment • Delivery of one-time password (OTP) by way of ATM • Security questions • Static or dynamic knowledge-based questions • New biometric or emerging technology that have not been approved by the Mastercard Identity Check™ global program owner. <p>NOTE: For regulated countries and regions like EUR, where Strong Consumer Authentication (SCA) is required for every authentication request, some of the authentication methods that are typically not allowed like static PINs and Knowledge based questions are allowed as the second factor provided a primary method of authentication is used as the first factor. For more information, refer to <i>Chapter 5, Identity Check Regional Program Requirements - EU</i>.</p>

NOTE: For a description of each compliant authentication method and the associated requirements, best practices, and security measures, refer to *Requirements for Authentication Methods* section.

Authentication Experience Requirements

Issuers, ACS providers, 3-D Secure servers, and merchants should encourage the best possible consumer experience.

As a best practice, when the experience cannot be rendered successfully on devices, an alternate experience should be provided.. The table below presents the requirements and best practices for issuers, ACS providers, 3-D Secure servers, and merchants.

Applicable To	Requirement and Best Practice
Issuers and ACS Providers	<p>Requirements</p> <ul style="list-style-type: none"> • Requirement 7: The issuer or ACS provider must prepare for the authentication experience to work without <ul style="list-style-type: none"> – Excessive customization (such as special fonts, custom colors, or images are not part of the authentication process for a wide range of devices). – Introductory pages that appear during shopping without a verification prompt. • Requirement 8: Authentication pages must contain the information necessary to allow the cardholder to authenticate and identify contact to call if there is a problem. • Requirement 9: The issuer or ACS provider must use the Mastercard® Identity Check™ logo on all authentication pages and on relevant enrollment sites as defined in the Mastercard Identity Check Artwork Usage Guidelines available on the Mastercard Brand Center. • Requirement 89: Only in the cases where a logo cannot be used due to technical limitations like non-support of graphics or special characters on feature phones (non-smart phones), Mastercard Identity Check shall be displayed in text as: “Mastercard® ID Check™” or “Mastercard ID Check” • Requirement 10: The issuer or ACS provider must recognize devices that it can and cannot support, and respond with an ARes message with a Transaction Status = U and Transaction Status Reason Code = 03 if the device is not supported. • Requirement 11: The issuer or ACS provider must make their FAQs regarding Identity Check available on their issuer website.

Applicable To	Requirement and Best Practice
	<p>Best Practice</p> <ul style="list-style-type: none"> The issuer or ACS provider should be prepared to receive transactions from multiple device categories and know how its screens will render on the device, before prompting for authentication. Browser flows should be designed to be similar or identical to app-based templates defined in the EMV 3-D Secure specification.

Applicable To	Requirement or Best Practice
Merchant and 3-D Secure Server	<p>Requirements</p> <ul style="list-style-type: none"> Requirement 12: For payment processors and acquirers, provide the proper identification of the authentication elements within the authorization message. (Specifically, accountholder authentication values [AAVs] must be provided in the authorization requests for both fully authenticated transactions and attempts.) Requirement 13: Display the Mastercard Identity Check identifier as described in the <i>Mastercard Identity Check Artwork Usage Guidelines</i> available on the Mastercard Brand Center. Requirement 14: Support a streamlined checkout experience by integrating a Mastercard Identity Check approved authentication flow.
Merchant and 3-D Secure Server	<p>Supported and Recommended</p> <ul style="list-style-type: none"> Merchant will only receive liability shift for transactions that have been submitted for authentication and receive a valid AAV. Transactions should be submitted with the proper Security Level Indicator in authorization, the authorization DE 48, subelement 42.

User Interface Requirements for App-based Transaction Flows

The App-based Transaction flows have user interface requirements described below.

Requirement 15: Mastercard Identity Check™ program requires that the SDK must display the Mastercard Identity Check logo on the processing screen during a Frictionless transaction.

NOTE: For more details on the User Interface requirements, refer to *EMV® 3-D Secure Core Specification*.

Key Performance Indicators—Compliance Measures

While delivering a favorable authentication experience, the addition of key performance indicators demonstrates the effectiveness of the authentication solution.

With the Mastercard Identity Check™ program, Mastercard strives to ensure the best-in-class authentication experience for issuers, merchants, and cardholders. This program aligns the Frictionless authentication experience with the key performance indicators to demonstrate the effectiveness of authentication. To ensure that authentication performs at optimum levels, Mastercard implemented the following measures for future compliance. These measures apply to issuers, merchants, 3-D Secure Servers, acquirers, and ACS providers.

Requirements	Key Performance Indicator	Issuer	ACS Provider	Acquirer	Merchant and 3DS Server
16	Overall e-commerce authorization approval rate for fully-authenticated Mastercard Identity Check transactions must not be below the global average of 90%.	X			

Requirements	Key Performance Indicator	Issuer	ACS Provider	Acquirer	Merchant and 3DS Server
18	Risk-based scoring solutions with a cardholder challenge strategy should not fail cardholder authentications (ARes status = N) at a rate exceeding 2%, unless there is a fraud attack.	X	X		
19	Risk-based scoring solutions without a cardholder challenge strategy should not fail cardholder authentications (ARes status = N) at a rate exceeding 7%.	X	X		
20	ACS and 3-D Secure Server vendor software must be available 99.0% of the time.		X		X

¹ Issuers that exceed a 7% decline rate for their risk-based solution over two successive months must remedy the situation by switching to a solution with a Challenge method.

Requirements	Key Performance Indicator	Issuer	ACS Provider	Acquirer	Merchant and 3DS Server
21	Merchants must complete processing of challenge authentication for 97% of Mastercard Identity Check transactions.				X
22	Acquirers must ensure that the authorization data remains compliant as outlined with the Data Integrity Program Edits.			X	

Privacy and Data Protection Matters

This section defines the terms used for privacy, data protection and information security matters in the Mastercard Identity Check™ program.

NOTE: For privacy and data protection requirements for Europe (GDPR), refer to Chapter 5 on regional specific requirements in this guide.

Definitions

Term	Definition
Controller	The entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

² This requirement allows for system errors.

Term	Definition
Data Subject Rights	Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making, and any other rights Data Subjects have to their Personal Data under Privacy, Data Protection and Information Security Requirements.
Personal Data	Any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity.
Process or Processing of Personal Data	Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of such data.
Processor	The entity which Processes Personal Data on behalf of a Controller.
Sub-Processor	Any Processor engaged (i) by the Processor or (ii) by any Sub-Processor of the Processor to process Personal Data on behalf of and in accordance with the instructions of the Controller or Processor.

Requirements

This section defines the requirements for privacy, data protection and information security matters in the Identity Check™ program.

NOTE: The term "Customer" used herein shall have the meaning ascribed to in the Mastercard Rules.

Category	Requirements
Privacy, Data Protection, and Information Security Requirements	<p>Requirement 23: All applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements relating in any way to the privacy, confidentiality, security and protection processing of Personal Data (“Privacy, Data Protection, and Information Security Requirements”), including, without limitation: Data Protection Act of 2018 (UK), the General Data Protection Regulation 2016/679/EU as amended or replaced from time to time and e-Privacy Directive 2002/58/EC as amended by Directive 2009/136/EC and their relevant EU national transposition legislation and implementation measures, including the recommendations and deliberations of the relevant data protection authorities; the Gramm-Leach-Bliley Act; laws regulating unsolicited email communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws regulating international data transfers and on-soil requirements, or both; laws regulating incident reporting and data breach notification requirements, including guidelines and recommendations from the competent regulators; the Fair Credit Reporting Act and similar state legislation; laws relating to the collection, storage, or other Processing of biometric data and biometric information; laws relating to the retention of Personal Data; law relating to banking secrecy and banking outsourcing; and all other similar international, federal, state, provincial, and local requirements; the Payment Card Industry Data Security Standards (PCIDSS); and all applicable provisions of a party's written information security policies, procedures, and guidelines must be adhered to.</p>

Category	Requirements
Compliance with Laws and Regulations	<p>Requirement 24: Mastercard and each Customer confirms and warrants that it complies with any and all applicable Privacy, Data Protection, and Information Security Requirements relating to the collection, use, disclosure, transfer and other Processing of Personal Data and that it will perform its obligations relating to Mastercard Identity Check in compliance with them. If any international, federal, state, provincial or local laws, rules, regulations, directives or governmental requirements are issued that impact, change, or supersede any material term or provision of this guide (collectively, Regulatory Requirement), then Mastercard and Customer mutually agree to modify this guide in a manner that is consistent with the intent and purpose of this guide and as necessary to comply with such Regulatory Requirement. Neither party shall unreasonably withhold its agreement to such modification. Should the Parties not be able to agree on such modifications within 30 days after the Regulatory Requirement is effective, then either party may upon written notice terminate this guide without any liability or fault.</p>
Subject to the Rules	<p>Requirement 25: Customer acknowledges that all information processed by Identity Check shall be deemed to be Confidential Information as defined in Rule 3.10 of the Mastercard Rules manual (or such successor rule).</p>

Category	Requirements
Legal Ground and Notice	<p>Requirement 26: Customer must rely on a valid legal ground, and must ensure that Data Subjects are properly informed in accordance with applicable Privacy, Data Protection, and Information Security Requirements relating to the collection, use, disclosure, transfer or otherwise Processing of Personal Data, the Processing of including sensitive or biometric data or the Processing for profiling or automated decision-making purposes, in the context of Mastercard Identity Check. In particular, Customer confirms and warrants that it will obtain consent for the collection, use, disclosure, transfers and any other Processing of Personal Data by Customer and Mastercard in the context of Mastercard Identity Check, to the extent and in the manner required by applicable Privacy, Data Protection and Information Security Requirements. Upon request from Mastercard, Customer must demonstrate that it relies on a valid legal ground for the Processing, including consent, where applicable. Customer also confirms and warrants that it will inform Data Subjects in particular of the transfer of their Personal Data to Mastercard in the United States, the ways in which their Personal Data will be Processed by Customer and Mastercard, any automated decision-making in the context of the Identity Check program and how Data Subjects can object to such automated decision-making, and any other information required by applicable Privacy, Data Protection and Information Security Requirements.</p>

Category	Requirements
Data Subject Requests	<p>In accordance with applicable Privacy, Data Protection, and Information Security Requirements:</p> <p>Requirement 27: Customer must develop and implement appropriate procedures for handling requests by Data Subjects to exercise their Data Subject Rights with regard to Personal Data Processed by Customer or Mastercard for the service (“Data Subject Requests”).</p> <p>Requirement 28: Where applicable, Customer must implement a process for allowing Data Subjects to withdraw their consent for the Processing of Personal Data and, to the extent applicable, for providing such opt-out requests to Mastercard without delay, as well as with respect to the implementation of any other choices that may be exercised by Data Subjects under the Customer's privacy notice and applicable Privacy, Data Protection, and Information Security Requirements.</p> <p>Requirement 29: Customer will be exclusively responsible for responding to any Data Subject Requests Mastercard or Customer may receive in the context of Mastercard Identity Check.</p> <p>Mastercard will inform Customer of any Data Subject Requests with respect to Personal Data that Mastercard or a Mastercard Sub-Processor received from that Customer's, and reasonably cooperate with that Customer in handling such request.</p>
Data Integrity	<p>Requirement 30: Customer is exclusively responsible for the accuracy, completeness, relevance and integrity of all Personal Data provided to Mastercard or to a Mastercard Sub-Processor.</p>

Category	Requirements
Government Requests for Data	<p>Requirement 31: Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, each of Mastercard and Customer shall promptly inform each other in writing if any competent authority, regulator or public authority of any jurisdiction requests disclosure of, or information about, the Personal Data that are Processed in connection with, in the case of Customer, the Mastercard Identity Check program, and in the case of Mastercard, any Personal Data of the Customer relating to the Mastercard Identity Check program.</p> <p>Requirement 32: Each party shall, without limiting its rights under applicable law, cooperate with the other parties as reasonably necessary to comply with any direction or ruling made by such authorities.</p>

Category	Requirements
Security	<p>Requirement 33: Customer and Mastercard must develop, implement, maintain and adhere to a comprehensive written information security program that complies with all applicable Privacy, Data Protection, and Information Security Requirements.</p> <p>Requirement 34: Without limitation, their information security program shall include technical, physical, administrative and organizational safeguards designed to (1) ensure the security and confidentiality of Personal Data; (2) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (3) protect against any actual unauthorized Processing, destruction, loss, alteration, use, disclosure or acquisition of or access to any Personal Data (“Information Security Incident”).</p> <p>Requirement 35: Customer and Mastercard must inform each other in writing in a commercially reasonable time frame, and in any event, no later than the time period required under applicable law, of any know Information Security Incident involving, in the case of Mastercard, any of Customer’s cardholders’ Personal Data processed for Identity Check, and in the case of Customer, any Personal Data processed through Identity Check.</p> <p>Requirement 36: Such notice shall describe, in reasonable detail, the nature of the Information Security Incident, the data elements involved, the identities of the affected individuals (if known), and the corrective action taken or to be taken to remedy the Information Security Incident.</p> <p>Requirement 37: Customer shall be solely responsible for any filings, communications, notices, press releases, or reports related to any Information Security Incident involving Personal Data processed by Customer or Mastercard in the context of the service.</p> <p>Requirement 38: Customer and Mastercard shall reasonably cooperate with each other in all matters relating to Information Security Incidents.</p>

Category	Requirements
Data Transfer and Storage	Requirement 39: To the extent applicable, Mastercard and Customer agree that they shall only transfer Personal Data outside of the country where it has been collected in accordance with the Privacy, Data Protection and Information Security Requirements.
Data Use	Requirement 126: Mastercard may use and disclose Personal Data for the purposes listed in 3.10 of Mastercard Rules in accordance with Privacy, Data Protection and Information Security Requirements. This may include disclosures to third parties (“Third Parties”) for the purposes of fraud, security and risk management, and product development related to those instances. In disclosing Personal Data to such Third Parties, Mastercard will require such Third Parties to protect the data with at least the same level of protection as set forth herein. Requirement 127: Each Participant must comply and must ensure that any other entity registered by Participant to comply with Privacy and Data Protection Requirements in connection with disclosing any Personal Data to Mastercard to allow the uses and disclosures described herein, including any laws and regulations requiring Participant or any other entity registered by the Participant to provide notices to individuals about information practices or to obtain consent from individuals to such practices.

Requirements for Authentication Method

This section describes the associated requirements, best practices, and security measures for the authentication method to consider when participating in the Mastercard Identity Check™ program.

For all cardholder authentication solutions, make sure the Identity Check identifier and mark is compliant with the usage guidelines provided on the Mastercard Brand Center.

Risk Based Authentication

A Risk Based Authentication (RBA) system examines each transaction using a risk scoring engine along with behavioral and transaction inputs to score a transaction all done in conjunction with an authentication solution such as Mastercard Identity Check™.

In a typical RBA deployment, depending on the risk assessment, the ACS can generate a fully authenticated AAV with or without the need to require the cardholder to authenticate themselves.

Requirement 40: When the issuer's ACS generates a fully authenticated AAV, regardless of the authentication method used, the issuer's ACS provider must generate the IAV, according to the Mastercard SPA algorithm. This includes utilizing the correct ECI value of 02 and control byte.

Requirement 41: Issuers must ensure that their ACS provider complies with the Mastercard ACS Compliance Program.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none"> • Requirement 44: Rejected or failed transaction message needs to include a customer service number or contact information. • Requirement 45: Issuer customer service agent must be able to ensure a rightful cardholder transaction is honored. 	<ul style="list-style-type: none"> • Maintain optimal rate for cardholder challenge. • Review and update risk engine rules model yearly. • Continued cardholder program awareness, even when a challenge event is infrequent. • Use machine device ID as an attribute to the risk engine. • Add additional attributes or sources of identity data as possible to minimize cardholder impact. • Email the cardholder promptly following declined transaction, inviting contact with issuer customer service. • Consider value of announcing this as fraud prevention program that will only affect cardholder when high-risk transactions are made. • Use this method as an interim solution until cardholders and authentication data are available for cardholder challenge when needed.

Biometric Authentication

When offering services that rely on the processing of biometric data, Customers should consider how to manage their privacy and data protection compliance obligations.

These may vary by jurisdiction and by the biometric modality. For more information on minimum compliance obligations, refer to Privacy and Data Protection section.

The following program requirements apply regardless of the biometric modality:

- **Requirement 47:** Cardholder should be notified and provide consent for use and storage of Personal Data.
- **Requirement 48:** Device ID must be part of solution.

For requirements specific to fingerprint, facial and voice recognition, refer to sections below.

Biometric—Fingerprint Match

Biometric fingerprint matching uses the cardholder fingerprint to authenticate the cardholder.

The cardholder's fingerprint is used during the provisioning process. During the purchase authentication, the cardholder is prompted to place a finger on the device to authenticate the authenticity of the cardholder.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none">• Requirement 49: Fingerprint match - must meet the requirements for Compliance Assessment and Security Testing (CAST).	<ul style="list-style-type: none">• The provisioning process should rely on issuer's online banking site or mobile app. Security questions not allowed.• It is recommended to ensure the cardholder privacy policy is compliant the Privacy, Data Protection and Information Security Requirements.• For detailed requirements and guidance on the management of sensitive biometric data on the CH device, refer to <i>Qualified Authentication Technologies for Consumer Digital Devices and Accessories-Overview; CAST Security Guidelines for Implementation</i>.

Biometric—Facial Recognition

Biometric facial recognition uses features of the face in combination with a 'liveness' test to authenticate the cardholder. Inclusion of the liveness test is to prevent spoofing.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none"> • Requirement 52: Facial Recognition - cardholder must be required to perform "liveness" testing, such as Eye blink. • Requirement 53: Facial Recognition - cycle time for verification must meet standard of 20 seconds or less. 	<ul style="list-style-type: none"> • It is recommended to ensure the cardholder privacy policy is compliant the Privacy, Data Protection and Information Security Requirements. • On-screen directions for photo taking, positioning, and lighting requirements. • The provisioning process should rely on issuer's online banking site or mobile app. Security questions not allowed. • High number of facial features captured for measurements is best. • For detailed guidance on the management of sensitive biometric data on the cardholder device, refer to <i>Qualified Authentication Technologies for Consumer Digital Devices and Accessories-CAST Security Guidelines for Implementation</i>. • For detailed requirements on false match and false reject rates, refer to <i>Qualified Authentication Technologies for Consumer Digital Devices and Accessories – Overview</i>.

Biometric—Voice Recognition

Biometric voice recognition identifies a person from characteristics of the voice to recognize the voice speaking.

At the time of provisioning, the cardholder's voice is analyzed for unique characteristics. At time of authentication, the cardholder is asked to repeat a phrase to authenticate themselves.

Required Elements/Performance Factors	Best Practices
<ul style="list-style-type: none"> Requirement 55: Voice recognition - cycle time for verification must meet standard. 	<ul style="list-style-type: none"> PC-based solutions should enable the cardholder to specify which number to have IVR dial. It is recommended to ensure the cardholder privacy policy is compliant the Privacy, Data Protection and Information Security Requirements. For detailed guidance on the management of sensitive biometric data on the cardholder device, refer to <i>Qualified Authentication Technologies for Consumer Digital Devices and Accessories-CAST Security Guidelines for Implementation</i>. For detailed requirements on false match and false reject rates, refer to <i>Qualified Authentication Technologies for Consumer Digital Devices and Accessories – Overview</i>.

Interactive Cards with PIN Pads

This solution uses a Mastercard certified interactive card, with a PIN to generate a one-time use code. The cardholder enters the one-time code during the authentication process.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none"> Requirement 57: Should be Mastercard approved interactive card. Requirement 58: The solution should be implemented as a secure element-based application. The solution will need server-side security requirements and code generation requirements to maintain synchrony with the cardholder device. 	<p>Cardholder education with issuance package.</p>

Push Notification Requesting Transaction Approval

The push notification requesting transaction approval from cardholder as out-of-band is a method that allows cardholders to authorize transaction using their mobile phones.

At the time of authentication, a push notification containing the transaction details from the mobile application is generated to the cardholder mobile device requesting the user to accept or reject the transaction.

The notification requires a tap to confirm or reject the purchase. If the user accepts the transaction, the confirmation message is sent to the issuer and the transaction is completed. If the user rejects the transaction, the transaction is stopped.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none"> • Requirement 59: The push notification requesting transaction approval must work with or on both smart phones and feature phones. • Requirement 60: The push notification requesting transaction approval must include bank name, merchant name, transaction amount, and currency. • Requirement 61: Cardholder must opt in to receive push notifications in accordance with applicable laws. • Requirement 62: The push notification requesting transaction approval should include a certificate validation application or device fingerprint. • Requirement 63: Push notification requesting transaction approval - the set-up for every out-of-band channel should be assessed for risk of compromise from Zeus and other man in the browser attacks. 	<ul style="list-style-type: none"> • Provide fallback method if notification times out. • Offer cardholder a second chance to confirm purchase by using an “Are you sure?” prompt. • Ensure that the push notification is converted to SMS to accommodate cardholders with feature phones.

Hand-held Token Generators/Fobs

The cardholder is prompted to generate an authentication token utilizing a bank issued token generator. This method often uses a PIN or requires the cardholder to insert an EMV® chip card to generate a one-time use code.

Requirements	Recommendations and Best Practices
<p>Requirement 64: Hand-held Token Generators/Fobs should require a PIN before generating dynamic number.</p>	<ul style="list-style-type: none"> • Cardholder education with issuance. • Reissuance practices in place if lost. • Provide fallback method. • Provide cardholder the ability to re-sync his or her devices and reset his or her own PINs. • May need server security requirements and code generation requirements, for example, unpredictability, to maintain synchrony between the server and the generator.

One-Time Passcode through SMS

A one-time use code is generated by the issuer or its ACS provider and delivered to the pre-designated cardholder mobile phone through a short message service (SMS) text. The cardholder then enters this code into the issuer authentication prompt displayed during the authentication process.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none">• Requirement 65: SMS message must include bank name, and transaction amount and currency.• Requirement 66: SMS OTP must expire 10 minutes after issuance and be good only for one purchase.• Requirement 67: SMS OPT - whichever out-of-band channel is used, the ways to set up that channel should be assessed for risk of compromise. For example, if the issuer web application can be used to set up SMS notifications, then Zeus and other man in the browser attacks are possible and should be mitigated.	<ul style="list-style-type: none">• Cardholder education at time of issuance.• Password should contain between six to eight digits, all numeric.• Include abbreviated merchant name if possible.• Only display last four digits of PAN in the body of the text message to confirm genuineness.• Issuers should proactively monitor SMS delivery failures to protect against large-scale delivery failures.

One-Time Passcode through Mobile App

One-time pass code is generated for cardholder use through a downloaded mobile application for this authentication solution. A one-time use code is generated by the mobile application, which is typically provided by the ACS provider.

The cardholder then enters this code into the issuer authentication prompt displayed during the authentication process. The provisioning process allows the cardholder to use the app for transactions which is critical to the success of this solution.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none"> • Requirement 68: OTP through Mobile Application, must expire 10 minutes after issuance and be good only for the specific purchase. • Requirement 69: PIN, code, gesture, or biometric check required to open the mobile application. • Requirement 70: OTP through Mobile Application; whichever out-of-band channel is used, the ways to set up that channel should be assessed for risk of compromise. If the issuer web application can be used to generate one-time passwords, then channels attacks are possible and should be mitigated. 	<ul style="list-style-type: none"> • Cardholder education at time of issuance. • Credential vetting on issuer's online banking site to precede activation of the mobile application. • Password should contain between six to eight digits, all numeric. • Only display last four digits of PAN.

Issuer Portal Verification

Re-directs cardholder to their issuer site for verification.

If an issuer does not want its ACS provider to manage any of its cardholder data or authentication processes, the issuer can use an issuer portal approach where the cardholder is instantly connected to the issuer's firewall site where credentials can be checked by the issuer only.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none"> • Requirement 72: Cardholder should not need to complete more than three screens. • Requirement 73: Issuer must ensure direct back to the merchant site is graceful and successfully completes. • Requirement 74: Issuer Portal verification whichever out-of-band channel is used, the ways to set up that channel should be assessed for risk of compromise. 	<p>Cardholder education at time of card issuance or sign up for banking site.</p>

Fallback Method Using Email

This Fallback method is an out-of-band method where the issuer forwards a one-time password and a customized authentication request to a cardholder's on-file email address

when he or she cannot use one of the primary authentication methods or fails them due to technical issues.

The cardholder must enter that one-time use passcode into the screen prompt in order to complete the transaction.

Requirements	Recommendations and Best Practices
<ul style="list-style-type: none"> • Requirement 75: Email should be recognizable to consumers as safe communications from their issuers or ACS (if ACS sending on behalf of issuer). • Requirement 76: Fallback method using email - must include bank name, merchant name, and transaction amount and currency. • Requirement 77: Fallback method using email - validity period of one-time password should be 10 minutes. • Requirement 78: Fallback Method using email, whichever out-of-band channel is used, the ways to set up that channel should be assessed for risk of compromise. If the issuer web application is used to set up email notifications, then Zeus and other man in the browser attacks are possible and should be mitigated. • Requirement 79: Email addresses must have Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) into to Domain Name Server (DNS) to ensure that the receiving email server validates the identity of the sending address to reduce the number of phishing or spoof emails. 	<ul style="list-style-type: none"> • The email message should have a customized heading with only last four digits of the cardholder PAN to assure cardholder that email is genuine. • The phone number for the customer service and the email address for the issuer should be included in the content of the email. • A consumer’s email address should not be displayed in full. Masking of the address is required. • The use of email to send a one-time password to the cardholder is not recommended. Email accounts can be compromised. At a minimum, the email on file used should not have been recently changed.

Payment Transactions

The Mastercard Identity Check™ program supports a regular e-commerce transaction along with various other use cases for Payment Transactions (PA). The requirements and recommendations associated with these are described below.

Regular e-Commerce Payment Transaction

A regular e-commerce payment transaction refers to any business transaction that involves buying and selling of goods and services, or both, or the transmitting of funds over the internet.

Details on how a regular e-commerce payment transaction is processed in Version 2.1 and version 2.2 of the spec respectively is illustrated in Appendix F - Payment Transaction Flow (Version 2.1 and 2.2).

Details on how a regular e-commerce payment transaction must be submitted in Authorization is listed in Appendix J - Regular E-commerce Payment Transaction—Authorization Data Elements.

NOTE: For regular e-commerce payment transaction, Authentication amount = Purchase amount.

3RI Payments

Version 2.2 of EMV™ 3DS Specification introduces 3RI payments, which offers the merchants the option to system-generate a payment transaction (channel = 3RI, Transaction type = PA) when the cardholder is not in session.

3RI payment transactions are also referred to as Merchant Initiated Transaction (MIT). 3RI payment transactions are highly beneficial for use cases like partial or split shipments, agent model, payments with unknown final amount, mail order or telephone order (MOTO) and recurring payments.

Requirement 128: A 3RI Payment transaction's 3DS Requestor Prior Transaction Authentication Data (Field Name: threeDSReqPriorAuthData) field must be used to reference the DS transaction ID of the initial authentication transaction (frictionless or challenge) the 3RI payment is tied to in use cases like partial/ split shipments, agent model, payments with unknown final amount and all recurring payments scenarios.

NOTE: The usage of all the elements in 3DS Requestor Prior Transaction Authentication Information (Field Name: threeDSRequestorPriorAuthenticationInfo) will increase ACS's chances of approving the transaction without requiring additional authentication.

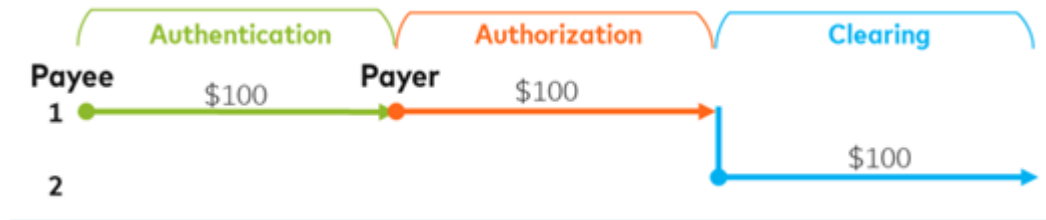
NOTE: For 3RI payment transaction use Authentication amount = Amount of the individual 3RI transaction.

Details on how a 3RI payment transaction (recurring and non-recurring) is processed in version 2.2 of EMV 3DS is illustrated in Appendix M - 3RI Payment Transaction Flow.

Delayed Delivery/Charged

This is a use case when for example, there is a trial of a product and payment is made after the trial period, or could be a pre-order of a product with payment before delivery.

Recommendation: Mastercard highly recommends that transaction is authenticated while the Cardholder is in-session and sent to authorization. Clearing is delayed until the time of delivery of product. This ensures a smoother process without requiring multiple authorizations or pre-authorizations or holding AAVs for extended periods. For example,

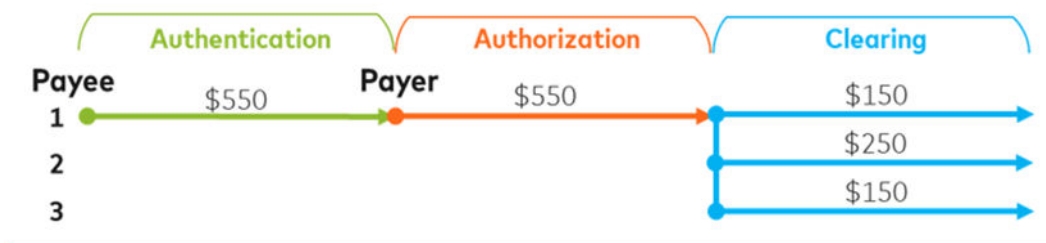


NOTE: For Delayed Delivery/Charged e-commerce payment transaction use Authentication amount = Purchase amount.

Partial Split Shipment

This is a use case when for example ordered products are not all available at the same time and the merchant decides to ship them separately.

Recommendation: Mastercard highly recommends that the transaction is authenticated for the full amount while the cardholder is in-session and sent to authorization for the full amount. Multiple clearing transactions are sent based on each of the shipments with the proper partial or final presentment message reason codes. This is in line with the best practices in the *Mastercard Customer Interface Specification for Authorization* manual. For example,

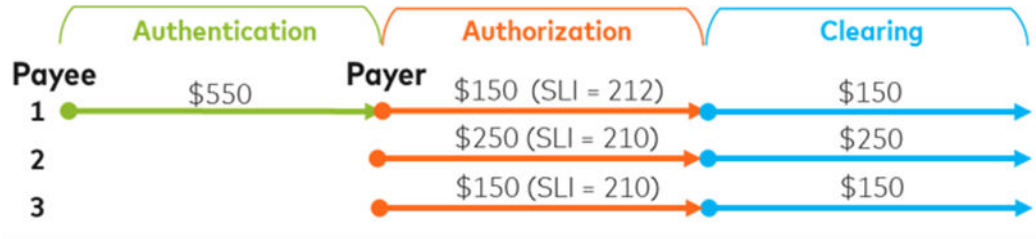


NOTE: For partial or split shipment transaction, Authentication amount = Purchase amount + capped partial shipment costs.

If the acquirer presents a separate authorization for each shipment including specific shipment costs, then this can be handled in two different ways based on the version of EMV 3DS being used

- Version 2.1: The transaction is authenticated for the full amount. The first authorization is submitted as a SLI = 212 (fully Authenticated) for the amount of the first shipment.

The Acquirer presents the authorization for each of the other shipments including specific shipment costs as a SLI = 210 (not authenticated) since Identity Check® does not allow re-use of AAVs in authorization (see requirement #104 in this document). For example,



- Version 2.2: The transaction is authenticated for the full amount. The first authorization is submitted as a SLI = 212 (fully Authenticated) for the amount of the first shipment. The subsequent shipments are authenticated as a 3RI Payment transaction for the shipment amount that generates a new AAV. The 3RI payment request for the subsequent shipments must reference the DS transaction ID of the initial or first fully authenticated payment transaction using the 3DS Requestor Prior Transaction Authentication data field. These subsequent shipments are then submitted into authorization as a SLI= 212 (fully authenticated) with their respective AAVs. For example,



Payment Initiated by a Different Merchant

This is a use case when the agent travel booking website manages booking or purchasing of airlines or hotels.

In such use cases, the consumer would buy a ticket for a certain airline (for example, Merchant1) at this travel website (for example, MerchantA).

For requirements around “Merchant Name” in AReq message for this use case Refer to Chapter 4, “*Mastercard Identity Check Required Data Elements*” section on IDC required data elements.

Agent Payment (with Multiple Merchants)

This is a use case when the agent travel website manages order of both hotel and airline for different merchants. In such use cases, there will be one authentication but multiple authorizations for each of the merchants.

Requirement: 90 The AAVs in both authorizations will be the same and must match the AAV in the authentication.

NOTE: For EU specific requirements and recommendations on this use case, refer to *Chapter 5, Identity Check Regional Program Requirements - EU*.

For example,



NOTE: For Agent model, Authentication amount = Total purchase amount

Version 2.2: With the usage of 3RI payment transaction, this scenario can be handled differently which can avoid the re-use of AAV and can also help with the name matching requirement between Authentication and Authorization for EUR. Below is an example of how it will work. The transaction is authenticated for the full amount. The first authorization is submitted as a SLI = 212 (fully Authenticated) for the amount of goods and services offered by merchant 1 (payee 1). The transaction for the merchant 2 (payee 2) is authenticated as a 3RI Payment transaction for the amount of good/ services offered by merchant 2, which generates a new AAV. The 3RI payment request for the second merchant must reference the DS transaction ID of the initial or first fully authenticated payment transaction using the 3DS Requestor Prior Transaction Authentication data field. All transactions are then submitted into authorization as a SLI= 212 (fully authenticated) with their respective AAVs. For example,



Unknown and Undefined Final Amount before Purchase

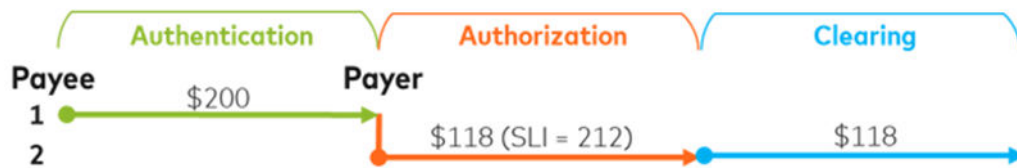
This is a use case when the payments are made on a travel turnstile, tips after a taxi ride, or when fines are accessed after a days or months of car rental.

In such use cases, the merchant sends an authentication request for the pre-agreed purchase amount plus the typical margin in business.

Recommendation: If the final transaction amount is higher, then it is recommended that an authentication request be made for the incremental amount.

If the cardholder is still in session, then an authentication request can be initiated for the incremental amount. If the cardholder is not in session then for version 2.1 of EMV 3DS, an authorization must be submitted for the incremental amount as SLI = 210 (not authenticated). For version 2.2 of EMV 3DS, 3RI payments can be used. For example,

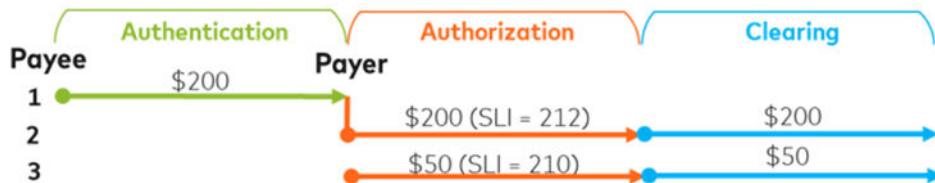
- If AuthE (USD 200) >= AuthO (USD 118)



- If AuthE (USD 200) < AuthO (USD 250)
 - Cardholder In-Session



- Cardholder Not in session Version 2.1



- Cardholder Not in session Version 2.2



Installment Payments

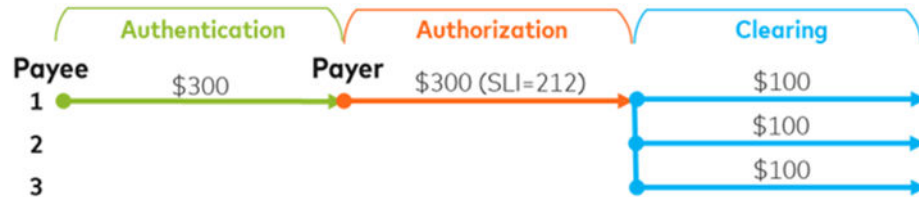
This is a use case when cardholder needs to pay for ordered goods in regular installments.

Requirement 91: An Installment Payment shall be indicated by the Merchant by the existing value 03 (= Installment transaction) in the existing 3DS Requestor Authentication Indicator field (Field Name: threeDSRequestorAuthenticationInd) of the Authentication Request (AReq).

Requirement 92: An Installment Payment shall be authenticated for the total value and does not require any further authentications.

Requirement 93: Authorization message must be submitted for the total value of the transaction. Multiple separate clearing transactions shall be submitted based on each of the installments with the proper partial or final presentment message reason codes.

NOTE: This is in line with the Mastercard transaction processing rules. It is the issuer's responsibility to not block the total authorization amount from the cardholder's open to buy limit. For example,



Refund of a Purchase

If an authenticated transaction (authorization or clearing) is reversed, canceled, or credited, there is no additional action required for authentication.

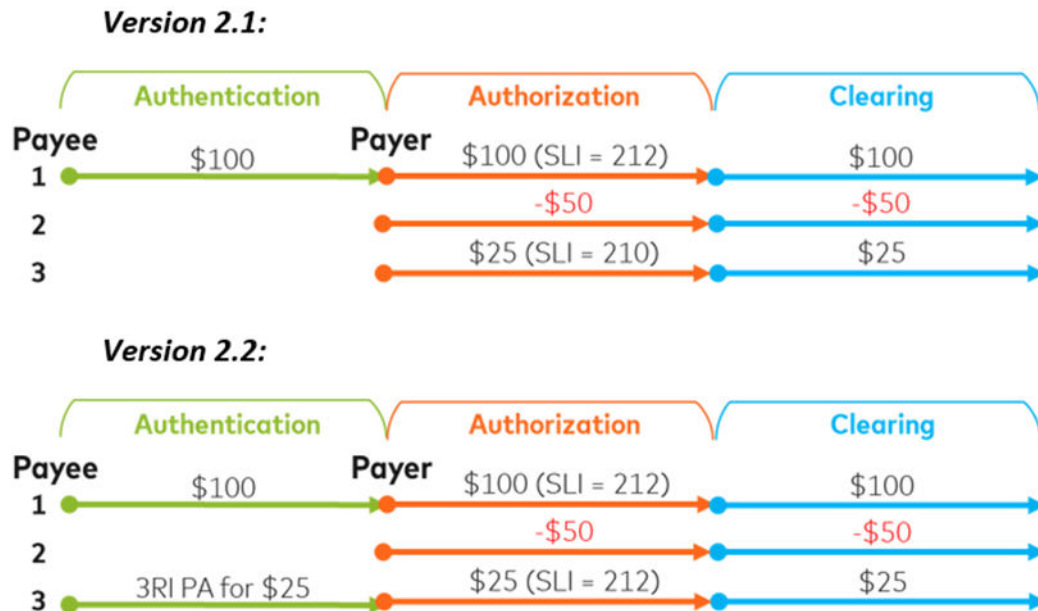
It goes through the BAU authorization and clearing flows, or both.

Replacement (Re-authorization) of a Refunded Purchase

Several merchants offer the option for consumers to return purchased goods. How or where the transaction is refunded, depends on how the original payment was made and the refund options offered by the merchant.

This is a use case when, for example, retailers allow cardholders to purchase items and offer free returns of products and goods cardholder does not want. The refunds are initiated even before merchant physically receives the returned goods and verifies. If the returned goods do not contain some of the actual merchandize that was supposed to be returned, then the merchant needs to be able to charge the consumer again for the missing goods.

With Version 2.1 of EMV 3DS, this can be achieved by submitting the transaction as a SLI = 210 (not authenticated) in authorization. With version 2.2 of EMV 3DS, the merchant can use 3RI payments transaction to authenticate for the amount that needs to get re-charged to the cardholder. Here is an example where the returned goods value is USD 50, and the missing goods are valued at USD 25. For example,



Adding Card-on-File—Regular Payment

Adding Card-on-File as part of a regular payment transaction is a use case when, for example, the cardholder is adding a card to their digital wallet as part of a regular purchase transaction.

The AReq for this payment transaction should have the following data elements and associated values.

- Message category = “01” (PA)
- 3DS Requestor Challenge Indicator = “03” (Challenge Requested: 3DS Requestor Preference) OR “04” (Challenge Requested: Mandate) for regulated markets
- 3DS Requestor Authentication Indicator = “04” (Add Card)

Adding Card-on-File—Recurring Payment

Adding Card-on-File as part of a recurring or installment payment transaction is a use case when, for example, the cardholder is adding a card to their digital wallet as part of the first transaction in a recurring payment or installment payment scenario.

The AReq for this payment transaction should have the following data elements and associated values.

- Message category = “01” (PA)
- 3DS Requestor Challenge Indicator = “03” (Challenge Requested: 3DS Requestor Preference) OR “04” (Challenge Requested: Mandate) for regulated markets
- 3DS Requestor Authentication Indicator = “02” (Recurring transaction) OR “03” (Installment transaction)
- Cardholder Account Age Indicator = “02” (During this transaction)

Requirement 149: An issuer ACS must challenge a request to add a Card-on-file (COF) regardless if it is requested using a non-payment or payment transaction.

Mail Order / Telephone Order (MOTO)

MOTO transaction is a card not present transaction where virtual terminal/payment software is used by merchants to manually key in consumers' payment information they receive over the phone, in the mail or through fax.

In EMV™ 3DS version 2.2, 3RI Indicator = 08 (Mail Order) or 09 (Telephone Order) is used to indicate a MOTO 3RI payment transaction.

In authorization, MOTO transactions are flagged by a value of 2 (Cardholder not present - mail/facsimile order) or 3 (Cardholder not present - phone or Automated Response Unit [ARU]) in DE61 SF4.

Flagging MOTO transactions in the correct way is the liability of the Merchant and the PSP/ acquirer.

Recurring Payments

Recurring Payments are where a merchant automatically charges a cardholder for specified goods or services without having to re-engage the cardholder (cardholder not present) until the predefined or agreed upon time frame (recurringExpiry) is reached.

Below are the Mastercard recommendations and requirements around recurring payments.

Requirement 94: A Recurring Payment shall be indicated by the merchant by the existing value 02 (= Recurring transaction) in the existing 3DS Requestor Authentication Indicator field (Field Name: threeDSRequestorAuthenticationInd) of the Authentication Request (AReq).

Mastercard highly recommends: a Strong Consumer Authentication (SCA) for the first transaction of the recurring payments. If SCA is used based on the recommendation above, the 3DS Requestor Challenge Indicator (Field Name: threeDSRequestorChallengeInd) field should contain the value of 03.

Mastercard highly recommends: a Strong Consumer Authentication (SCA) after the Recurring Expiry date is reached and the next set of recurring payments need to be initiated. The maximum limit before another SCA is needed (recurringExpiry) is between merchant and cardholder. This agreement is typically made before the authentication screens.

Recommendation: As a best practice, merchants should have a recurring expiry associated with all recurring transactions after which SCA should be initiated, but in cases like subscriptions where there is no established expiry or end date of recurring transactions, merchants should indicate the value of "99991231" (YYYYMMDD format) in the "recurringExpiry" field.

Recommendation: Recurring payments with a variable frequency can set the recurringFrequency to '1' to indicate that the frequency of payments is not set.

For EMV 3DS version 2.1.0 and lower, all subsequent transactions that are part of a recurring payments go straight to authorization.

NOTE: For EU specific requirements and recommendations on this use case; refer to *Chapter 5, Identity Check Regional Program Requirements - EU*.

The table below lists some of the key required data elements that are used for processing recurring payments (initial, or first, transaction as well as subsequent transactions) for Version 2.1 of EMV 3DS.

Table 9: Use Case: Recurring Payments

3DS Version	Network	TXN Type	Description	
			Data Element	Values
2.1	Authenticati on	Initial/First Recurring Txn	Message Flow	AReq
			Message Category	01- PA
			Device Channel	01- App, 02 - Browser
			Request Message (AReq)	
			3DS Requestor Authentication Indicator	02 =Recurring transaction
			3DS Requestor Challenge Indicator	03 = Challenge requested (3DS Requestor preference)
			Response Message (ARes)	
			Transaction Status	Y
			ECI 02 or 07	AAV leading Indicator kA (if frictionless) or kB (if challenged) with ECI= 02 kO (if frictionless) or kP (if challenged) with ECI= 07

NOTE:

The ECI = 07 and the leading indicators kO and kP have been specially introduced for recurring payments. The usage of these for the initial recurring transaction is at the discretion of the ACS Issuer, but we highly recommend it.

3DS Version	Network	TXN Type	Description	
			Data Element	Values
NOTE: For details around transaction processing, refer to <i>Processing Matrix</i> section in Chapter 4.				
		Subsequent Recurring Txn	Subsequent recurring transaction do not go through authentication as card holder is not in session and a 3RI payment flow is not supported in V2.1.	
NOTE: Liability for this transaction is with the merchant.				

Version 2.2 of EMV 3DS supports 3RI payments and this allows the subsequent recurring transactions to be submitted to authentication. The table below lists some of the key required data elements that are used for processing recurring payments (initial/first transaction as well as subsequent transactions) for example, Version 2.2 of EMV 3DS.

Table 10: Use Case: Recurring Payments

3DS Version	Network	TXN Type	Description	
			Data Element	Values
2.2	Authenticati on	Initial/First Recurring Txn	Message Flow	AReq
			Message Category	01- PA
			Device Channel	01- App, 02 - Browser
			Request Message (AReq)	
			3DS Requestor Authentication Indicator	02 =Recurring transaction
			3DS Requestor Challenge Indicator	03 = Challenge requested (3DS Requestor preference)
			Response Message (ARes)	
			Transaction Status	Y
			ECI	02 or 07
			AAV leading Indicator	kA (if frictionless) or kB (if challenged) with ECI= 02 kO (if frictionless) or kP (if challenged) with ECI= 07

3DS Version	Network	TXN Type	Description	
			Data Element	Values
<p>NOTE: The ECI = 07 and the leading indicators kO and kP have been specially introduced for recurring payments and are required to be used for subsequent recurring 3RI payment transactions. The usage of these for the initial recurring transaction is at the discretion of the ACS Issuer.</p>				
<p>NOTE: For details around transaction processing, refer to <i>Processing Matrix</i> section in Chapter 4.</p>				
		Subsequent Recurring Txn	Message Flow	AReq
			Message Category	01- PA
			Device Channel	03- 3RI
			Request Message (AReq)	
			3DS Requestor Authentication Indicator	02 =Recurring transaction
			3RI Indicator	01 = Recurring transaction
			3DS Requestor Prior Transaction Authentication Data	DS Transaction ID of the Initial or first recurring payment transaction.
			NOTE: The presence of DS transaction ID in the 3DS Requestor Prior Transaction Authentication Data field is a requirement for 3RI payment transactions for recurring payments. Refer to the 3RI payments section of this document for more information on the requirement.	
			Response Message (ARes)	
			Transaction Status	Y
ECI	07			
AAV leading Indicator	kO (if frictionless) or kP (if challenged using de-coupled authentication)			

3DS Version	Network	TXN Type	Description	
			Data Element	Values
<p>NOTE: The ECI = 07 and the leading indicators kO and kP have been specially introduced for recurring payments. Their usage in subsequent recurring 3RI payment transactions is mandatory.</p>				
<p>NOTE: For details around transaction processing, refer to <i>Processing Matrix</i> section in Chapter 4.</p>				

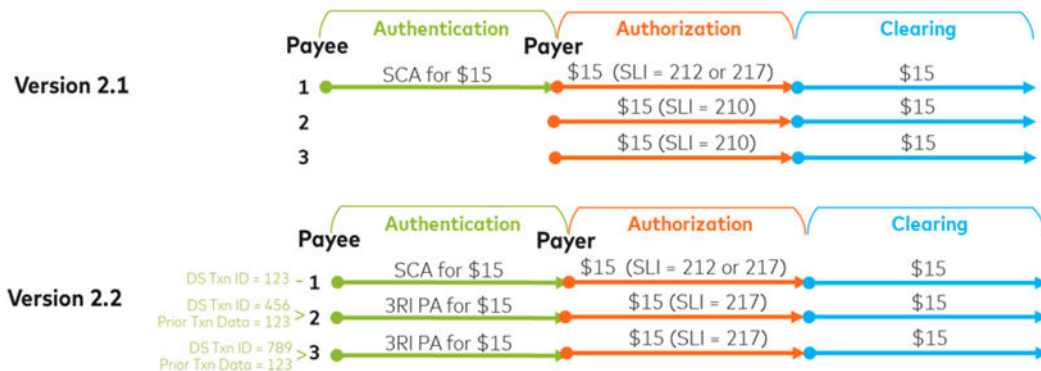
Detail recommendation on how initial and subsequent recurring transactions should be submitted in Authorization is listed in Appendix K - Recurring Payment Transaction—Authorization Data Elements.

There are different types of recurring payments use cases. Below are some examples along with any specific recommendations or requirements for the given use case.

Recurring Payment with Fixed Amounts

This is a use case when, for example, there is monthly Newspaper or streaming service subscription.

Below is an example of how this use case will be handled in version 2.1 and 2.2 based on the guidelines and requirements above.

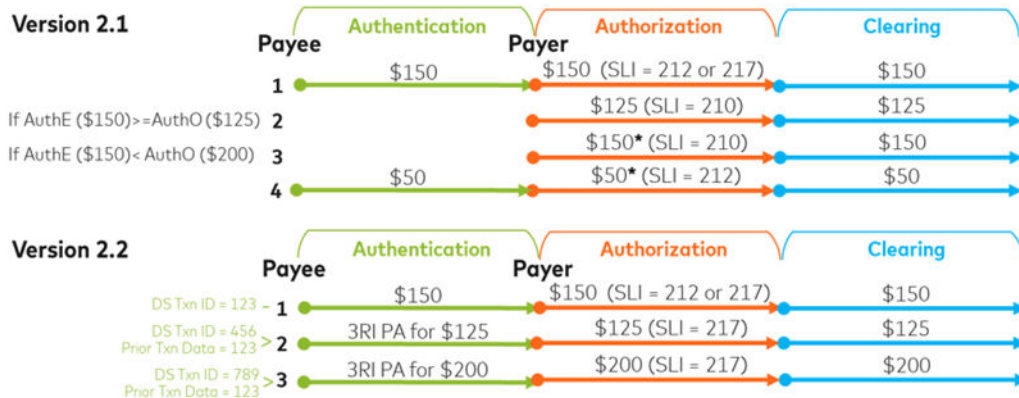


Recurring Payment with Variable Amounts

This is a use case when for example, there are monthly mobile top-up or utility payments with the amount varying every month.

The Merchant sends an EMV 3DS authentication request for the maximum amount in business or a typical margin in business and must be an amount that the Cardholder would reasonably expect. This ensures that the final authorization amount is less than or equal to the authentication amount.

*If the authorization amount exceeds the authenticated amount by more than 20%, it is recommended that Merchants treat the incremental amount compared to the authenticated amount as a separate transaction if the cardholder is in session. For Europe, this transaction for incremental amount may require a separate Strong Customer Authentication unless an exemption applies. If the cardholder is not in session then the transaction is submitted as a 210.

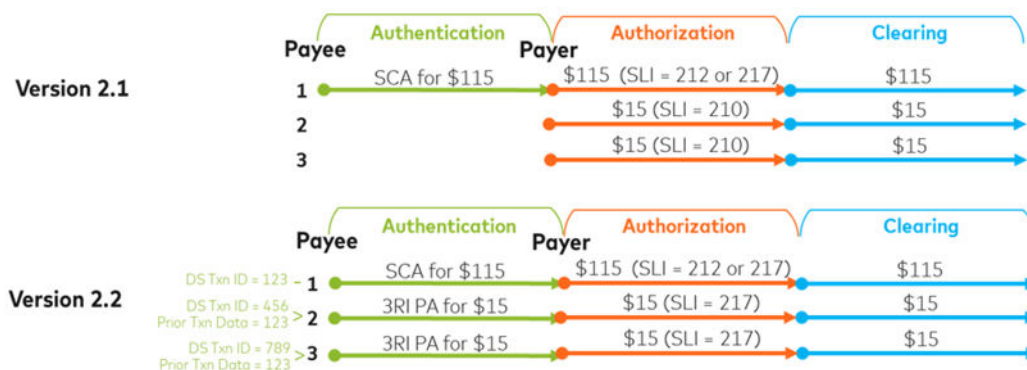


Recurring Payment Combined with One-time Purchase

This topic is about recurring payments that are combined with one-time purchases (also known as mixed cart).

This is a use case when for example, Monthly video streaming service subscription with price of decoder in initial transaction. In the example below, cost of decoder = USD 100 and the monthly subscription = USD 15.

- Transaction 1: purchaseAmount = Purchase amount + subscription amount.
- Transaction 2, Transaction N: purchaseAmount = subscription amount



Recurring Payment with Fixed Limit and Threshold

This topic is about recurring payment with fixed limit and threshold (individual or corporate) but variable frequency and amounts.

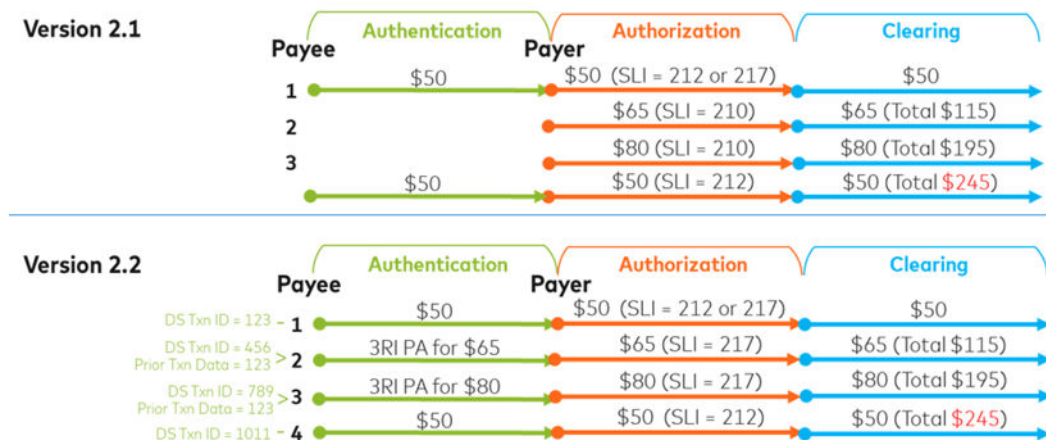
This is a use case when, for example, there is a credit line up to a certain amount for online web or cloud services.

In the below example the consumer is signing up for USD 200 worth of services. The messaging to tell consumer that they are signing up for USD 200 worth of services should happen before the authentication page. The first transaction would be the authentication of the amount for the first 'bill' to the consumer (USD 50 in this case) and not USD 200 even though that is the agreed upon amount of that service contract between the Merchant and the Cardholder.

Subsequent SCAs and new recurring 'agreement' will be required when the agreed limit has been reached. The authentication amount for subsequent SCAs will be the transaction amt. In this case, a Merchant-initiated exemption or re-authentication will be needed. Re-authentication may leverage exemptions, whitelisting, and decoupled authentication.

Merchant will also need to initiate a separate communication (not part of authentication page) with consumer to sign another service agreement for an agreed upon amount.

The tracking of amount in each transaction and calculation of when the agreed limit is reached is done by the issuer. It is critical that the subsequent transactions contain the prior or first transaction information to allow issuer to keep track. If not present, it is issuer decision to do SCA or decline the transaction.



Use of Account Status Inquiry (ASI) in Recurring Payment

In certain recurring payment scenarios, authorization may not occur within seven days of the authentication.

In these scenarios, Mastercard highly recommends that after an authentication has occurred, an Account Status Inquiry (ASI; (DE61 SF7 = 8 identifies an ASI in authorization)) should be sent by the merchant or acquirer to the issuer in authorization. An ASI can carry the related authentication data (DS transaction ID, AAV with corresponding

leading indicator, and security level indicator). This is a way to inform the issuer that a successful authentication took place for that transaction. This is particularly useful in regions like Europe where there are mandates regarding strong consumer authentication (SCA) in relation to a recurring payment and MIT agreement.

The first true authorization message for such a transaction can also contain the same AAV as the ASI. Any subsequent authorizations shall not contain the same AAV.

NOTE: For more information on refreshing AAVs beyond their 10-90 day validity period, refer to the "AAV Refresh" section.

Non-Payment Transactions

The Mastercard Identity Check™ program supports various use cases for Non-Payment Authentication (NPA) transactions. The requirements and recommendations associated with NPA are described below.

NPA flows support functions where there is no financial transaction (purchase of goods or services) but the 3-D Secure requestor still needs to communicate to the ACS issuer to validate a cardholder. It is still a card based transaction for example, cannot use bank account number, passport number, or other such identifiers.

Mastercard does not offer any Attempts or Stand-in RBA services for non-payment transactions. The most common use cases of non-payment transactions is cardholder verification as part of the below items.

- Add card to a wallet*
- White list verification
- Account creation without payment
- Tokenization*

*These functions can also be performed through a payment transaction.

For the non-payment transaction flows for version 2.1 and 2.2 of EMV 3DS, refer to Appendix G - Non-Payment Transaction Flow (Version 2.1 and 2.2).

Mastercard highly recommends NPA app and browser transactions to be stepped up to encourage deterministic authentication. It is the issuer's decision to do so, or not, as they assume the liability.

Requirement 95: For EMV® 3DS version 2.1.0, all 3DS Requestor Initiated (3RI) NPA transactions must be frictionless including the 'AAV Refresh' transactions.

Requirement 96: NPA authentications shall not be submitted for authorization except in the case of 'AAV Refresh' transactions.

Requirement 97: No AAV shall be generated for NPA transactions except in the case of 'AAV Refresh' transactions.

Requirement 98: An ECI (N0 = Not authenticated or N2 = Authenticated) and the Transaction Status Reason code shall be included in the ARes and RReq message for NPA.

Adding Card-on-File (outside of a payment transaction) This is a use case when for example the cardholder is adding a card-on-file to a digital wallet of their choice without the intention of initiating a purchase transaction at that time. The AReq for this 'add card' non-payment transaction should have the following data elements and associated values

- Message category = "02" (NPA)
- 3DS Requestor Challenge Indicator = "03" (Challenge Requested)
- 3DS Requestor Preference) OR "04" (Challenge Requested: Mandate) for regulated markets
- 3DS Requestor Authentication Indicator = "04" (Add Card)

NOTE: For adding card-on-file, refer to requirement 149 for rule regarding step-up/challenge.

Chapter 4 Liability Shift and Processing Matrix

This section describes the liability shift rules and the required elements for transaction processing.

Liability Shift Rule Summary.....	98
Transaction Processing Matrix.....	98
Accessing the Processing Matrix File.....	99
Mastercard Identity Check Transaction Processing Requirements.....	100
Mastercard Identity Check Required Data Elements.....	105

Liability Shift Rule Summary

Issuers should always check the *Chargeback Guide* for the current liability shift rules.

Liability Shift Descriptions

There are two types of liability shifts, merchant only (also known as "Attempts"), and fully authenticated, which are described below.

- Merchant only (also known as Attempts)—this liability shift describes when only the merchant is participating in an authentication program. The 3-D Secure server contacted the Mastercard Directory Server™ for authentication services and
 - the issuer's account range does not participate in an authentication program
 - the cardholder is not enrolled in the authentication program
 - the ACS cannot be reached, or
 - the ACS responds with a transaction status that does not meet program usage guidelines.
- Fully authenticated—this liability shift describes when both the merchant and the issuer participate in an authentication program and the issuer ACS has had the opportunity to authenticate the cardholder and provide a fully authenticated proof of authentication.

For a Mapping of Payment Transaction Status, ECI, SLI, SPA 2 AAV Leading Indicators & Transaction Liability, refer to Appendix L - Transaction Status, SLI, and Liability Mapping.

Transaction Processing Matrix

The transaction processing matrix shows the flow of relevant data elements as they progress through the transaction life cycle: authentication, authorization, and finally, clearing.

Authentication is the first step in protecting the cardholder. Authentication is the process of identifying the cardholder, prior to authorization. The results of the authentication are included in the authorization to help create a trusted transaction between merchant, acquirers and issuers. Often the authentication data passes through many downstream processes and is necessary for authorization and clearing data. Understanding how the data is passed from one entity to another is imperative to ensure accuracy of the end results.

Mastercard® has enhanced edits for authorization and clearing data to ensure accurate data is passed before program benefits can apply. In addition, issuers are required to validate the AAV (either themselves or using the on-behalf service) for all authorization transactions, including Stand-In.

The enhanced authorization edits **downgrade** the Security Level indicator in the authorization request when the AAV is not valid. The enhanced clearing will edit reject the clearing message when the security level of the authorization and the clearing message

are not in sync. For further processing details, refer to *Customer Interface Specifications*, *IPM Clearing Formats* or *Single Message System Specifications* manuals.

NOTE: The liability shift assignment is a function of the clearing process.

Refer to the application reference manuals such as *Customer Interface Specification* for authorization; *IPM Clearing Formats* for clearing; and the *Chargeback Guide* for additional details on the liability shift and required elements for processing.

Refer to Appendix L - Transaction Status, SLI, and Liability Mapping for a Mapping of Payment Transaction Status, ECI, SLI, SPA 2 AAV Leading Indicators and Transaction Liability.

Accessing the Processing Matrix File

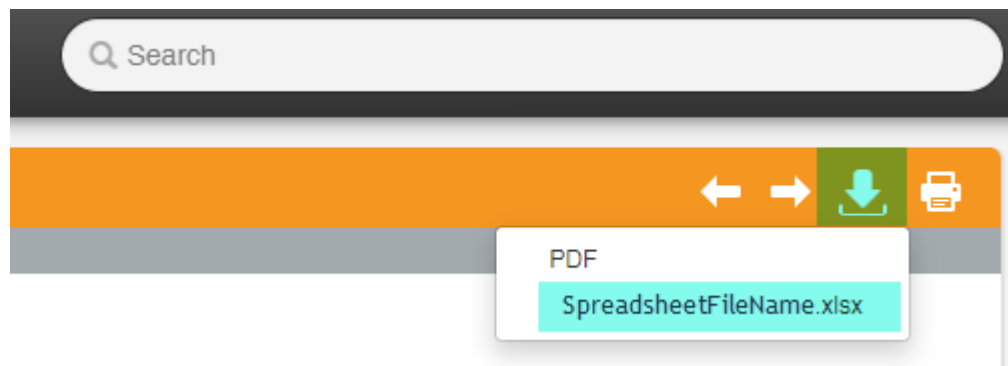
The Mastercard Identity Check Processing Matrix file is a spreadsheet attachment in Microsoft Excel® file format. It outlines the processing flow of data elements from authentication, Authorization and clearing.

About this task

Follow the instructions below to access the file; this file can be saved to a local drive for later use.

Procedure

1. From the **HTML edition** of this document, click the file download icon in the upper right corner.



2. Click the spreadsheet file name under the drop down arrow.
 3. When the file opens, save it to a location on your computer.
- OR**
4. From the downloaded **PDF edition** of this document, click the **paperclip** and then click the spreadsheet file name.



5. When the file opens, save it to a location on your computer.

NOTE: Before printing this document, be aware that this spreadsheet is large; check your printer settings and paper selection.

Mastercard Identity Check Transaction Processing Requirements

The sections below detail the Mastercard specific processing and data element requirements that are part of the Mastercard Identity Check™ implementation of EMV® 3-D Secure.

Multiversion Support

The Mastercard DS currently supports version 2.1 of EMV 3DS. Support for future announced versions of EMV 3DS (version 2.2) will follow the EMVCo timeline.

Requirement 144: All ACSs and 3DS Servers must not only support the EMVCo specification version they are certifying for, but also every lower or previous version that may be still 'active or current' according to EMVCo.

All the parties in the EMV 3DS ecosystem must comprehend how multiple versions of the EMV 3DS specification will be supported especially when all not parties that are part of a transaction (Merchant, 3DS Server, DS and ACS) are on the same version.

According to the EMV 3DS specification, the 3DS Server is required to determine the version that all components parties will use. In adherence to the EMV 3DS specification, if Mastercard DS receives a message with a version that the DS AND the ACS (both) do not support, then the DS will error out, as it is expected that the 3DS Server must have determined this before sending the transaction.

If a 3DS Server wants to avoid getting errors from DS, the 3DS Server should be able to determine the appropriate message version that both the DS and the ACS support before creating the AReq (refer to section on Preq/PRes Processing).

The table below provides a matrix of the different scenarios with multiple versions and the expected behavior.

Scenario	Merchant	3DS Server	DS	ACS	What happens
A1	2.1	2.1	2.1	2.1	BAU processing
A2	2.1	2.1	2.1	2.2	3DS Server determines minimum common denominator (between DS and ACS) and requires merchant to submit on V1 (2.1.0) - Areq = 2.1.0
A3	2.1	2.1	2.2	2.1	3DS Server determines minimum common denominator and requires merchant to submit on V1 (2.1.0) - Areq = 2.1.0
A4	2.1	2.2	2.1	2.1	If Merchant is V1 (2.1.0) 3DS Server creates a Areq = 2.1.0
A5	2.2	2.1	2.1	2.1	N/A - Merchant cannot have 2.2.0 if 3DS Server doesn't support since Merchant codes to API their 3DS server provides them spec for and supports. Areq = 2.1.0
A6	2.1	2.1	2.2	2.2	3DS Server cannot support and are not certified to create 2.2 msg. Areq = 2.1.0
A7	2.1	2.2	2.1	2.2	3DS Server determines minimum common denominator and requires merchant to submit on V1 (2.1.0) - Areq = 2.1.0
A8	2.2	2.1	2.1	2.2	N/A - Merchant cannot have 2.2.0 if 3DS Server doesn't support since Merchant codes to API their 3DS server provides them spec for and supports. Areq = 2.1.0
A9	2.1	2.2	2.2	2.1	3DS Server determines minimum common denominator and requires merchant to submit on V1 (2.1.0) - Areq = 2.1.0
A10	2.2	2.1	2.2	2.1	N/A - Merchant cannot have 2.2.0 if 3DS Server doesn't support since Merchant codes to API their 3DS server provides them spec for and supports. Areq = 2.1.0
A11	2.2	2.2	2.1	2.1	3DS Server determines minimum common denominator and requires merchant to submit on V1 (2.1.0) - Areq = 2.1.0
A12	2.2	2.2	2.2	2.2	BAU processing. The 3DS Server gives the option for the merchant to submit either 2.1.0 or 2.2.0 since all other systems will be supporting both
A13	2.2	2.2	2.2	2.1	3DS Server determines minimum common denominator and requires merchant to submit on V1 (2.1.0) - Areq = 2.1.0
A14	2.2	2.2	2.1	2.2	3DS Server determines minimum common denominator and requires merchant to submit on V1 (2.1.0) - Areq = 2.1.0
A15	2.2	2.1	2.2	2.2	N/A - Merchant cannot have 2.2.0 if 3DS Server doesn't support since Merchant codes to API their 3DS server provides them spec for and supports. Areq = 2.1.0
A16	2.1	2.2	2.2	2.2	If Merchant is V1 (2.1.0) 3DS Server creates a Areq = 2.1.0

PREq/PRes Processing

The PREq message is sent from the 3DS Server to the DS to request information about the Protocol Version (one or more) supported by available ACSs and the DS and if one exists, any corresponding 3DS Method URL. The PRes message is the DS response to the PREq message. The 3DS Server can use the PRes message to cache information about the Protocol Version (one or more) supported by available ACSs and the DS, and if one exists, about the corresponding 3DS Method URL. This message set is not part of the 3-D Secure authentication message flow.

The data in the PRes will be organized by card range as configured by a DS. The information provided on the Message Version Number (one or more) supported by ACSs can be used in both the App-based and Browser-based flows.

The 3DS Server formats a PREq message and sends the request to the DS in one of two ways

1. **Entire list request:** If this is the first time that the cache is being loaded (or if the cache has been flushed and needs to be reloaded, or if the DS does not support partial cache updates), the Serial Number data element is not included in the request, which will result in the DS returning the entire list of participating card range information.
Recommendation: Due to the size of the file and associated potential performance issues, it is recommended that 3DS Servers request the entire list only when required and not more than only once in a 24 hour period.
2. **Delta request:** Otherwise, the 3DS Server should include the Serial Number from the most recently processed PRes message, which will result in the DS returning only the changes since the previous PRes message. The DS manages the Serial Number to ensure that the response to a PREq message for a particular Serial Number includes all updates posted since that Serial Number was issued. If the Serial Number provided in the PREq message is invalid (for example, if too old and can no longer be found), the response will be an Error Message with an Error Code = 307. If the PREq message does not include a Serial Number, the DS PRes message response shall contain all card range entries.

The following card ranges will be included on the PRes which should route to the Mastercard DS.

- All ranges enrolled in IDC
- All active Mastercard ranges not enrolled in IDC
- Token ranges
- Pay By Bank Account (PBA) card ranges

NOTE: This will not change the format of data elements provided on the PRes. This will only add new card ranges to include on the PRes.

When the 3DS Server formats a PReq message without a serial number and sends the request to the DS, the DS retrieves all the card ranges and updates the PRes to add all the active Mastercard card ranges so that the 3DS server will receive all the eligible card ranges. While updating the PRes, all the card ranges will have an action indicator of “A” for ADD and the latest Serial Number for response is updated in the PRes.

When 3DS Server makes a subsequent request with a serial number, the DS will calculate the Delta (changes for all ranges updated since that Serial Number was issued only) and include them in PRes.

Delta is not needed for PwBA card ranges. All the PwBA card ranges will be included in the PRes in both full feed and delta requests.

For eligible card ranges, the Preparation Response (PRes) may reflect a 19-digit card range which may map back to a 16-digit PAN. Due to this scenario, we have the following program requirement:

Requirement 153: When leveraging the PRes data provided by the Mastercard Directory Server to determine participating account numbers in either a preparation flow or an authentication flow, 3DS servers must use the full card range data when determining eligibility of an account number. Eligibility should not be determined solely on the BIN (that is, 6, 8, 9, or 11 digit value).

3DS servers must also consider the following:

- A 16-digit PAN provided by a requestor may fall within a 19-digit account range provided in the PRes data. For example, PAN provided by a requestor: "230XXX*****2" (16 digits) PRes card range data: "230XXX000000000000-230XXX999999999999" (19 digits)
- Therefore, if the 3DS Server is unable to map a 16-digit PAN to a corresponding 16-digit account range, the 3DS Server may need to validate that such PAN does not fall within a 17, 18, or 19- digit range.
 - New logic will validate if the 16-digit PAN falls within a 19-digit account range.
 - If not found then validate if the 16-digit PAN falls within an 18-digit account range.
 - If not found then validate if the 16-digit PAN falls within a 17-digit account range.

Mastercard DS Processing Requirements

- **Requirement 80:** An issuer ACS is not permitted to respond with an ARes transaction status = A.
The ACS receives an Error message for the AReq transaction Status = A and the transaction routes to Mastercard Stand-in RBA.
- **Requirement 81:** The read timeout threshold is 3000ms and the connection timeout threshold is 10000ms. Mastercard Stand-in RBA will be used to provide a fully authenticated value or a merchant-only authentication value when ACS is unavailable.
- **Requirement 82:** All Merchants and 3-D Secure servers must use the PReq/PRes messages for checking what EMVCo version is supported by the card range.
- **Requirement 84:** An issuer ACS is not permitted to respond with a RReq transaction status of
 - RReq Status = A
 - RReq Status = CIn the event this occurs, the ACS receives an error message and Mastercard Stand-in RBA is used to provide a fully authenticated value or a merchant-only authentication value.
- **Requirement 99:** SPA2 AAV must be generated for all EMV 3DS Identity Check payment transactions.
- **Requirement 140:** 3DS server shall submit all authentication messages to the Mastercard DS when the transaction is sent to Mastercard for authorization (either for 3DS1 or 3DS2). 3DS Servers shall not bypass the DS and send requests directly to the ACS.
- **Requirement 145:** If a cardholder is not enrolled, an issuer ACS must only respond with transaction status = N with reason code = 13, so that Mastercard Smart Authentication Stand-In can be utilized. No other reason code should be used unless strong consumer authentication (SCA) is required.

NOTE: If the acquirer BIN and Merchant ID combination sent to the DS does not match the combination that was enrolled while on-boarding with Identity Check then Mastercard DS will send error code 303. For more information about onboarding and enrollment processes, refer to [Mastercard Identity Check Onboarding Guide for Acquirers, Merchants, Operators, and 3-D Secure Service Providers](#).

- **Requirement 147:** ACS shall respond with Transaction Status = “R” (Authentication/ Account Verification Rejected; Issuer is rejecting authentication/verification and request that authorization not be attempted) in the case the authentication fails and the transaction cannot be submitted to authorization.

Authorization Requirements

- **Requirement 85:** All issuers must validate the AAV at the time of authorization either via the Mastercard AAV validation service or the issuer's self validation service. This applies to all authorizations including Stand-in.

For SPA 2 AAV technical specifications refer to the SPA2 AAV for Identity Check Program available on Mastercard Publications.

NOTE: If the issuer enrolls in the Mastercard AAV validation Service (OBS 05/06) then Mastercard only validates the Mastercard portion of the SPA2 AAV. Mastercard will not validate the IAV part of the SPA2 AAV.

- **Requirement 102:** DS transaction ID must be populated in the authorization message for all payment transactions sent to the Mastercard Authentication network (EMV 3DS).
- **Requirement 103:** Program Protocol ID must be populated in the authorization message for all payment transactions sent to the Mastercard Authentication network (EMV 3DS) (1 for 3D Secure Version 1.0 (3DS 1.0), and 2 for EMV 3-D Secure (EMV 3DS, aka 3DS 2.x)).
- **Requirement 104:** Same AAV shall not be reused in multiple authorization messages except for the agent use case, where the authentication and purchase is made on an agent site (like a combined travel booking of airline and hotel) but the authorizations are for separate merchants.
- **Requirement 118:** Transaction Amount - The amount in the authorization (or the total or accumulated amount of all authorizations relating to a single authentication, for example, in the case of split shipments) has to be lower than or equal to the amount in the authentication for all electronic remote card-based payment Card Not Present (CNP) transactions for which the merchant sent an authentication request. The Mastercard validation service tolerates authorization amount being +20% of authentication amount as a maximum threshold before the transaction is considered non-compliant.

Recommendation: If the transaction amount is not known in advance, the authentication amount must be an amount that the cardholder would reasonably expect, that is, within an acceptable tolerance. Identity Check program recommends +20% tolerance. In this case, if the authorization amount exceeds the authenticated amount, it is recommended that merchants treat the incremental amount compared to the authenticated amount as a separate transaction which can be authenticated through normal 3DS rails if cardholder is in session or through 3RI payments if cardholder is no longer in session.

Requirement 129: The authentication amount for a card not present (CNP) Transaction must use the same currency as the authorization.

Recommendation: All issuers should use the Digital Transaction Insights (DTIs) as part of their transaction approval decisioning process.

Requirement 148: Merchants shall not submit a transaction to authorization if that transaction received a “R” as Transaction Status in the authentication response.

Requirement 150: Issuers must not systematically decline EMV 3DS transactions with Security Level Indicator (SLI) = 211.

Requirement 151: Issuers must have an approval rate of 90% or higher for EMV 3DS transactions with Security Level Indicator (SLI) = 212.

Clearing Requirements

Requirement 86: For all payment transactions sent to the Mastercard Authentication network (EMV 3DS), the Clearing messages must adhere to the following *IPM Clearing Formats*.

- PDS 0052 (Electronic Commerce Security Level Indicator) must match DE 48, subelement 42 of the authorization otherwise the clearing message will be rejected with reason code 2806
- PDS 0185 (Accountholder Authentication Value) must match DE 48, subelement 43 of the authorization
- PDS 0186 (Program Protocol) must match DE 48, subelement 66, subfield 1 of the authorization
- PDS 0184 (Directory Server Transaction ID) must match DE 48, subelement 66, subfield 2 of the authorization

NOTE: Airlines are exempt from sending DS transaction ID and Program Protocol fields in Clearing until the updates are made to the T960 file.

NOTE: Merchant Name - The name in clearing can be different than in Authorization or Authentication and should not be changed to comply with current rules as stated in Chapter 5 of this guide.

Recommendation: For the agent use case, it is recommended that merchant names in the clearing message contains the agent name and a reference to the merchant or merchants of the different transactions so that the transaction can be easily recognized by the Cardholder and dispute resolution is not initiated for transaction not recognized by the Cardholder.

Mastercard Identity Check Required Data Elements

This section contains requirements and recommendations around data elements that are required for Mastercard Directory Server (DS) for each of the 3-D Secure Messages.

Only data elements that are required beyond the ones mentioned in the EMV[®] 3-D Secure specification or that have Identity Check specific requirement or recommendation are mentioned below.

For a complete list of all required data elements refer to the EMV[®] 3-D Secure specification ([EMVCo](#)).

NOTE: All data elements that have acceptable values defined, the DS will only allow the standard values defined in the EMV 3-D Secure specification. Values defined as reserved for future use by either EMVCo or DS will not be allowed.

Table 11: Authentication Request Message (AReq)

Data Element	Field Name	Mastercard Rules and Recommendations
3-D Secure Requestor Authentication Information	threeDSRequestorAuthenticatio nInfo	Recommendation: Mastercard recommends that data be sent if the Requestor would like to help provide the best possible data to assist with Risk Based Authentication. Inclusion of this data could allow the transaction to qualify as strong authentication from prior logon to app/wallet.
3-D Secure Requestor ID	threeDSRequestorID	<p>Every 3DS Server will be assigned a Mastercard DS defined requestor ID prefix at time of onboarding. This prefix will be of length = 9 alphanumeric characters and will end with an underscore (_).</p> <p>Requirement 105: Requestor ID format must be: 'DS defined prefix for 3DS server_3DS server defined ID'.</p> <p>Recommendation: 3DS server defined ID for merchant connecting directly to the 3DS Server, could be Merchant's MID.</p> <p>Requirement 106: 3DS server defined ID for scenario where merchants are connected through third parties, PSP, Gateways, Merchant Aggregators, and so forth. must be such that 3DS Server is able to identify the parties down to the merchant level.</p> <p>NOTE: Special characters cannot be used within the requestor ID at this time. The only special character allowed is an underscore (_).</p>

Data Element	Field Name	Mastercard Rules and Recommendations
3-D Secure Requestor Name	threeDSRequestorName	<p>Requirement 107: This name must be in the format: '3DS Server name_requesting entity'.</p> <p>Requirement 108: The '3DS Server name' must match the name registered in the Mastercard DS at time of onboarding (3DS Server Company Name).</p> <p>Requirement 109: The 'requesting entity' can be name of merchant connecting directly to the 3DS Server, or name of 3rd party/PSP/ Gateway/ Merchant Aggregator's (whichever is applicable).</p> <p>NOTE: Special characters cannot be used within the requestor ID at this time. The only special character allowed is an underscore (_).</p>
3-D Secure Server Operator ID	threeDSServerOperatorID	Requirement 110: 3-D Secure Server Operator ID field is required by the Mastercard DS.
Acquirer BIN	acquirerBIN	If the acquirerBIN/merchantID combination in the incoming message to the DS does not match what is enrolled with DS, then DS will respond with error code 303 on the ARes message.
Acquirer Merchant ID	acquirerMerchantID	
Card/Token Expiry Date	cardExpiryDate	Requirement 111: Card/Token Expiry Date field is required by Mastercard DS.
DS Reference Number	dsReferenceNumber	This field is populated by the DS and sent to the ACS. 3DS Server does not need to populate this field in the AReq.

Data Element	Field Name	Mastercard Rules and Recommendations
Merchant Name	merchantName	Requirement 112: This name must match the name registered in the Mastercard DS at time of enrollment. In use cases where the transaction is initiated by a different merchant, like in the case of a travel agent site managing booking for airlines or hotels, the name must follow the following format: 'Travel agent name_merchant (hotel or airline) name'
Message Category	messageCategory	The Mastercard DS will allow the standard EMV 3-D Secure values as well as the value of 80. The DS will not allow other values defined as reserved for future use by either EMV or DS.
Message Extension	messageExtension	This field is required in specific Mastercard offerings as described in this guide.
Merchant Risk Indicator	merchantRiskIndicator	Recommendation: These 2 data elements from the Merchant Risk Indicator field should be sent as part of the AReq message - Delivery Timeframe (deliveryTimeframe) and Shipping Indicator (shipIndicator). Recommendation: It is strongly recommended to send all the other detailed data elements that are part of the Merchant Risk indicator field as well.

Table 12: Authentication Response Message (ARes)

Data Element	Field Name	Mastercard Rules and Recommendations
ACS Operator ID	acsOperatorID	Requirement 113: ACS Operator ID field is required by Mastercard DS
ACS URL	acsURL	The Mastercard DS will not maintain multiple ACS URLs. If the first URL attempted is not available, then the DS will attempt an immediate retry. Upon second failure, the DS will Stand-in on behalf of ACS and send an appropriate Stand-in RBA response to the 3-D Secure Server.
Electronic Commerce Indicator	eci	Requirement 114: Electronic Commerce Indicator (ECI) field is required by Mastercard DS for ARes and RReq messages and must be sent for all transaction statuses (A, N, R, U, and Y).
Transaction Status Reason	transStatusReason	Requirement 115: Transaction Status Reason field is required in ARes for Non- Payment Authentication (02-NPA). It is required if the Transaction Status (transStatus) field = N or U. For Payment authentication (01- PA), refer to requirements in EMVCo specification.

Table 13: Results Request Message (RReq)

Data Element	Field Name	Mastercard Rules and Recommendations
Authentication Type	authenticationType	The DS will not allow the standard EMV value of 01.

Data Element	Field Name	Mastercard Rules and Recommendations
Transaction Status Reason	transStatusReason	Requirement 116: Transaction Status Reason field is required in RReq for Non- Payment Authentication (02-NPA). It is required if the Transaction Status (transStatus) field = N or U. For Payment authentication (01- PA), refer to requirements in EMVCo specification.

Mastercard sends different error codes when a required, conditional, or optional field is formatted incorrectly or is sent as an empty string, null, or is missing entirely. The table below summarizes the errors that will be triggered in these conditions:

For a field if	Required field	Not applicable for that Message type/OR device channel message category combo	Conditional field who has met conditional requirement	Conditional Field which is present even when Conditional requirement recognized by DS is not present	Optional field
"FieldName"":"	Send 201	Ignore and drop the field before sending to next component.	Send 201	Send 203	Send 203
"FieldName"":n ull"	Send 201	Ignore and drop the field before sending to next component.	Send 201	Send 203	Send 203
Entire field is missing	Send 201	Ignore and drop the field before sending to next component.	Send 201	Go ahead and forward the message to next component	Go ahead and forward the message to next component

For a field if	Required field	Not applicable for that Message type/OR device channel message category combo	Conditional field who has met conditional requirement	Conditional Field which is present even when Conditional requirement recognized by DS is not present	Optional field
Format incorrect	send 203	Ignore and drop the field before sending to next component.	Send 203	Send 203	Send 203

Chapter 5 Identity Check Regional Program Requirements - EU

This section describes the requirements for the Mastercard Identity Check™ Program for the European region.

Privacy and Data Protection – Europe.....	113
Revised Payment Service Directive (PSD2) Requirements.....	119
Strong Customer Authentication.....	119
Soft Decline or Decline as SCA Required	119
PSD2 SCA Exemptions and Maestro	120
Dynamic Linking.....	120
Biometric Authentication Support.....	121
Auto-enrollment.....	122
Mandated Support for EMV 3-D Secure.....	122
Acquirer Strong Consumer Authentication (SCA) Exemption	122
Low-Value Payments and Management of Counters.....	124
Merchant Fraud Rate.....	124
Acquirer Country Code.....	124
Secure Corporate Payments Exemptions	125
Merchant Whitelisting.....	126
Recurring Payments/MITs.....	127
Mastercard Services in Support of PSD2 RTS	128
Mastercard On-Behalf AAV Validation Service.....	128
Authentication Express (Europe).....	128

Privacy and Data Protection – Europe

This section applies to the Processing of Personal Data of Data Subjects subject to EU Data Protection Law in the context of the Mastercard Identity Check™ Program (the “Program”).

The terms used in this section have the meaning set forth in this section. Capitalized terms not otherwise defined herein have the meaning given to them in the Program Guide.

This section supplements the privacy and data protection terms contained in Chapter 3 “Privacy and Data Protection Matters” of this Program Guide, the Early Adoption Program agreement or otherwise agreed between the Parties, to the extent they pertain to the Processing of Personal Data subject to EU Data Protection Law. In case of a conflict, the provisions of this section will prevail. For the avoidance of doubt, the Mastercard Rules remain in full force and effect except as modified below.

1. The following terms have the meanings set out below for this Section:

Definitions 1.1

“EU Data Protection Law” means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the European Economic Area (“EEA”) countries (as amended and replaced from time to time).

1.2

“Europe” means the Enhanced Enrollment Agreement (EEA) countries, that include: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

1.3

“GDPR” means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).

1.4

“Mastercard Binding Corporate Rules” (or ‘Mastercard BCRs’) means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available at <https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf>.

1.5

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

2. Roles of the Parties

For the purpose of the Schedule, the parties acknowledge and confirm that:

2.1

Mastercard is a Controller for the Processing of Personal Data to build authentication and fraud models;

2.2

Participating Merchants and Issuers (altogether “Participants”) are Controllers and Mastercard is a Processor for the application of the Mastercard authentication and fraud models to cardholder authentication requests and the Processing of resulting authentication scores and factors.

2.3

Notwithstanding the above, Participants acknowledge and agree that Mastercard may Process Personal Data for any purpose listed in Section 3.10 of the Mastercard Rules, to the extent they apply, including internal research, fraud, security and risk management

2.4

Participating 3DS Service Providers represent and warrant that they (a) act as Processors of the participating Issuers or Acquirers on whose behalf they Process Personal Data in the context of the Program; (b) received a mandate from such Issuers or Acquirers to enter into these Terms and Conditions on behalf of such Issuers or Acquirers; and (c) are authorized by such Issuers or Acquirers to receive cardholder authentication information from Mastercard via the Program and Process that information on behalf of such Issuers or Acquirers.

2.5

Participating Acquirers represent and warrant that they (a) act as Processors of the participating merchants on whose behalf they Process Personal Data in the context of the Program; (b) received a mandate from such merchants to enter into these Terms and Conditions on behalf of such merchants; and (c) are authorized by such merchants to enroll them to the Program or to otherwise facilitate merchants performing authentication requests (d) where applicable, Process Personal Data on behalf of such merchants.

2.6

This Schedule does not create any joint-controllership relationship between any of the parties.

3. Obligations of the Parties Each party must comply with EU Data Protection Law when Processing Personal Data as stipulated in Clause 3. Each party will: (i) cooperate with the other party to fulfill their respective data protection compliance obligations under EU Data Protection Law; (ii) take all security measures required pursuant to EU Data Protection Law, and at the minimum, the measures listed in Annex 2; and (iii) take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation. In addition, Participants will be responsible for ensuring a valid legal ground for Processing, providing notice to Data Subjects, and complying with Data Subject Rights, with regard to all Processing of Personal Data under these Terms and Conditions, including the Processing for which Mastercard is a Controller.

4. Obligations of Participants Notwithstanding Clause 4, each Participant represents and warrants that, when it acts as a Controller, it will:

4.1

Only give lawful instructions to Mastercard when Mastercard acts as a Processor.

4.2

Rely on a valid legal ground for each Processing activity listed in Clause 3, including obtaining Data Subjects' consent if required or appropriate under EU Data Protection Law.

4.3

Provide appropriate notice to the Data Subjects regarding (1) the Processing of Personal Data, in a timely manner and at the minimum with the elements required under EU Data Protection Law, (2), as appropriate, the existence of Processors located outside of Europe and of the Mastercard BCRs, including the Data Subjects' right to enforce Mastercard BCRs as third-party beneficiaries (by linking to the Mastercard BCRs).

4.4

Inform Mastercard in writing of any Data Subjects' requests to exercise their Data Subject Rights, and respond to such requests in consultation with Mastercard, except when Mastercard acts as Participant's Processor in which case Participant is not required to inform Mastercard of such requests and Participant will be solely responsible for responding to such requests in accordance with EU Data Protection Law.

4.5

Comply with any applicable requirements under EU Data Protection Law if it engages in automated decision-making or profiling in the context of the Program.

**5.
Obligations
of
Mastercard**

Mastercard confirms and warrants that, when it acts as a Processor, it complies with the Mastercard BCRs, and that it:

5.1.

Only Processes Personal Data in accordance with the Participant's lawful written instructions and not for any other purposes than those specified in Annex 1, Clause 3, the Mastercard Rules, or as otherwise agreed by both Parties in writing

5.2

Will promptly inform Participant if, in its opinion, the Participant's instructions infringe EU Data Protection Law, or if Mastercard is unable to comply with the Participants' instructions.

5.3

Cooperates with the Participant to fulfil the Participant's own data protection compliance obligations under EU Data Protection Law, including by providing all information available to Mastercard as necessary to demonstrate compliance with the Participant's own obligations and where applicable to help the Participant in complying with its Personal Data Breach notification obligations and conducting data protection impact assessments or prior consultation with supervisory authorities.

5.4

Assists the Participant in fulfilling its obligation to respond to Data Subjects' requests to exercise their Data Subject Rights, and notifies the Participant about such requests if Mastercard receives them directly from the Data Subject.

5.5

Notifies the Participant when local laws prevent Mastercard (1) from fulfilling its obligations under this Schedule or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by this Schedule or the Mastercard BCRs, and (2) from complying with the instructions received from the Participant via this Schedule, except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Participant is responsible for notifying its competent supervisory authority as applicable and required under EU Data Protection Law.

5.6

When Terms and Conditions expire or upon termination of the Terms and Conditions or upon a request to delete or return Personal Data by the Participant, Mastercard will, at the choice of the Participant, delete, anonymize, or return all the Personal Data to the Participant, and delete or anonymize existing copies unless applicable law prevents it from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case Mastercard will protect the confidentiality of

the Personal Data and will not actively Process the Personal Data anymore).

6. Data Transfers In relation to its Processing of Personal Data in the context of the Program, each party may transfer Personal Data outside of Europe in accordance with EU Data Protection Law, and Mastercard may transfer Personal Data outside of Europe in accordance with the Mastercard BCRs or with any other lawful data transfer mechanism that provides an adequate level of protection under EU Data Protection Law. Mastercard represents and warrants that it will abide by the Mastercard BCRs when Processing Personal Data in the context of the Program.

7. Data Disclosures **7.1**
The parties represent and warrant that they will only disclose Personal Data Processed in the context of the Program in accordance with EU Data Protection Law, and in particular that they will require the data recipients to protect the data with at least the same level of protection as in these Terms and Conditions

7.2

Mastercard represents and warrants that it will only disclose Personal Data in accordance with the Mastercard BCRs.

7.3

When Mastercard acts as a Processor, Participants give a general authorization to Mastercard to Process and sub-Process Personal Data to internal and external Sub-Processors in connection with the Program under the conditions set forth below and Mastercard represents and warrants that when sub-Processing the Processing of Personal Data in connection with the Program, it:

7.3.1

Binds its internal Sub-Processors to respect Mastercard BCRs and to comply with the Participant's instructions.

7.3.2

Requires its external Sub-Processors, via a written agreement, to comply with the requirements of EU Data Protection Law applicable to processors and data transfers, with the Participant's instructions and with the same obligations as are imposed on Mastercard by this Schedule and the Mastercard BCRs, including sub-Processing and audit requirements set forth in Mastercard BCRs.

7.3.3

Remains liable to the Participant for the performance of its Sub-Processor's obligations.

7.3.4

Commits to provide a list of Sub-Processors to the Participant upon request.

7.3.5

Will inform the Participant of any addition or replacement of a Sub-Processor in a timely fashion so as to give the Participant an opportunity to object to the change or to terminate its registration for the Program before the Personal Data is communicated to the new Sub-Processor, except where the Program cannot be provided without the involvement of a specific Sub-processor.

8. Data Protection and Security Audit

8.1.

Each party commits to conduct audits on a regular basis to control compliance with EU Data Protection Law, including the security measures provided under Clause 4 and Annex 2, and Mastercard to control compliance with the Mastercard BCRs. Upon prior written request, each party agrees to cooperate and within reasonable time provide the requesting party with: (a) a summary of the audit reports demonstrating its compliance with EU Data Protection Law obligations and this Schedule, and as applicable Mastercard BCRs, after redacting any confidential and commercially sensitive information; and (b) confirmation that the audit has not revealed any material vulnerability, or to the extent that any such vulnerability was detected, that such vulnerability has been fully remedied.

8.2.

When Mastercard acts as a Processor, Mastercard agrees to cooperate and within reasonable time provide the Participant acting as the Controller with: (a) a summary of the audit reports demonstrating Mastercard's compliance with EU Data Protection Law obligations under this Schedule and Mastercard BCRs, after redacting any confidential and commercially sensitive information; and (b) confirmation that the audit has not revealed any material vulnerability in Mastercard's systems, or to the extent that any such vulnerability was detected, that Mastercard has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with EU Data Protection law and Mastercard BCRs or reveal some material issues, subject to the strictest confidentiality obligations, Mastercard allows the Participant acting as the Controller to request an audit of Mastercard's data protection compliance program by an external independent auditor, which is jointly selected by the parties. The external independent auditor cannot be a competitor of Mastercard, and the parties will mutually agree upon the scope, timing, and duration of the audit. Mastercard will make available to the Participant acting as the Controller the result of the audit of its data protection compliance program.

9. Applicable Law and Jurisdiction

The parties agree that this Schedule and the Processing of Personal Data will be governed by the law of Belgium and that any dispute will be submitted to the Courts of Brussels.

Revised Payment Service Directive (PSD2) Requirements

The Second Payment Service Directive is a revised version of the original Payment Service Directive (PSD).

It focuses on electronic payments and is a directive that applies to payment services in the European Union (EU) and the EEA countries. This section describes Identity Check™ Program requirements and recommendations as it relates to PSD2.

Strong Customer Authentication

Strong Customer Authentication (SCA) increases security of a transaction, by requiring consumers to use two-factor authentication to identify themselves. The two factors can be categorized as knowledge, possession or inherence. SCA is to be applied as according to PSD2 RTS requirements.

Requirement 117: SCA shall be required according to PSD2 requirements and as described in the Authentication Guidelines for Europe.

Requirement 130: The “3DS Requestor Challenge Indicator” field must always be filled by the merchant to avoid any doubt or confusion about the challenge needs for the transaction.

NOTE: For more information on SCA, refer to *Appendix A, Mastercard Authentication Best Practices*.

Soft Decline or Decline as SCA Required

An issuer may decline an authorization request (especially in the case of no 3DS authentication) and indicate to the merchant or acquirer that SCA is required.

The issuer will do this by returning a response code of 65 (RC65 - Exceeds withdrawal count limit) in DE39 of the authorization response.

For European rules related to this topic, refer to the *Transaction Processing Rules (5.8 Authentication Requirements for PSD2)*.

Recommendation: Until all issuers support RC65, merchants are recommended to always send an authentication request following an authorization that was declined for non-financial and non-technical reasons.

NOTE: If merchants go straight to authorization, the authorization must be done during checkout, that is, before goods are actually shipped (clearing has to wait until shipment). This will be critical in the soft decline scenario, as the authentication following the soft decline will require SCA to occur while the cardholder is still in-session.

PSD2 SCA Exemptions and Maestro

There are three special programs enabling European online and e-commerce merchants to accept Maestro™ transactions without 3DS. They are in the below list.

- Maestro Low Merchant Risk Program (MLRMP)
- Maestro Utility Payment Program (MUPP)
- Maestro Recurring Payment Program (MRPP)

MLRMP, MUPP and MRPP participating merchants are subject to eligibility and operations requirements that are specified in the Europe Operations Bulletin December 2011 and Europe Region Operations Bulletin March 2016.

MLRMP, MUPP and MRPP participating Merchants use specific values. These specific values are peculiar to these special Maestro programs and they are not used for Mastercard

- SLI 213
- Mastercard-assigned Merchant ID
- Static AAV

NOTE: From the PSD2 RTS on SCA effective date, the above Maestro specific values will come to an end (SLI 213, Mastercard-assigned Merchant ID, static AAV).

Requirement 131: From the PSD2 RTS on SCA effective date, European online and e-commerce merchants who want to accept Maestro transactions without Strong Customer Authentication will be able to do so only if an RTS regulated exemption applies.

Requirement 132: From the PSD2 RTS on SCA effective date, merchants who want to leverage Acquirer SCA exemptions must follow the same use cases and specifications for Mastercard and for Maestro.

Dynamic Linking

Dynamic linking is a requirement of PSD2, that provides guidelines and rules around linking of transactions between authentication and authorization.

This makes the authentication layer stronger as these requirements counter malicious attacks where transaction details could be altered after the transaction is authenticated but before it is authorized. When the RTS comes into force, Dynamic Linking will be required.

The below is a requirement that needs to be met as part of dynamic linking:

The Merchant name and authentication amount shall be shown to the Cardholder during the authentication experience, on the Merchant page (controlled by the 3-D Secure Server) and on the authentication page (controlled by the ACS).

Mastercard Identity Check™ recommendations in support of these requirements are:

Recommendation: During the setup of the Recurring Payment, the ACS needs to clearly display the message “Please authenticate this recurring payment for the following amount:

___” (fill in amount including currency) or similar and display the Recurring Payment amount plus merchant name to avoid cardholder confusion.

For global requirement on transaction amount, refer to Requirement 118.

In cases where the final amount is unknown in advance follow the recommendation found in Chapter 4, *Mastercard Identity Check Transaction Processing Requirements*, Authorization requirements.

Recommendation: In addition to the global recommendation referenced above, for transactions subject to PSD2 RTS, the transactions for the incremental amount may require a separate Strong Customer authentication unless an exemption applies or unless they are handled as Merchant Initiated Transactions (MIT). If the transaction amount exceeds the cardholder’s ‘reasonable expectations’, the refund right for authorized transactions under Articles 76-77 PSD2 may apply.

For European rules on currency between Authentication and Authorization, refer to the *Transaction Processing Rules and Procedures* (5.8 Authentication Requirements for PSD2).

For European rules regarding merchant name, refer to the *Transaction Processing Rules and Procedures* (chapter of Merchant Location).

These rules help cardholders to recognize the merchant name during the authentication and help comply with PSD2 dynamic linking regulation which requires the merchant name to be shown to the Cardholder and issuer during authentication to ensure that the authentication code (AAV) is linked to the merchant.

Since ACSs and fraud prevention tools often rely on the merchant’s name to assess the fraud risk, this also helps to avoid fraud in cases where fraudulent merchants try to re-use the name of a large and trusted merchant.

Using unique merchant names also can help to reduce authentication abandonment if the trusted beneficiary (Merchant Whitelisting) exemption is used, because many issuers will identify whitelisted merchants by their merchant name used during the authentication.

Biometric Authentication Support

Issuers are mandated to offer cardholders biometric authentication in most European countries depending on the country.

For rules related to biometric authentication support along with the effective dates, refer to the *Mastercard Rules* (Chapter 6.1 - Card Issuance).

NOTE: This rule is not applicable for co-brand partners, as issuers cannot be forced to auto-enroll these types of co-brand portfolios.

Auto-enrollment

Depending on the issuer country, the support of auto-enrollment is either mandated or strongly recommended in Europe.

For rules related to auto-enrollment along with the effective dates, refer to the *Mastercard Rules* (chapter 6.1 - card issuance).

Mandated Support for EMV 3-D Secure

Before EMV® 3-D Secure and Identity Check Program are mandated depending on the issuer country, merchants can only use EMV 3-D Secure if the issuer is enrolled in EMV 3-D Secure.

If the issuer is not enrolled in EMV 3-D Secure, merchants need to fall back to 3-D Secure 1.0.

For acquirers that have been mandated to support EMV 3-D Secure, merchants need to fall back to 3-D Secure 1.0.

At this point in time, Mastercard has not announced the end of the liability shift for 3-D Secure 1.0.

For details around the mandate, applicable countries and effective dates, refer to the *Transaction Processing Rules* (Chapter 5.8.1) and *Mastercard Rules* (Chapter 6.1).

Requirement 124: Issuers should not decline transactions only because 3-D Secure 1.0 is used by the merchant or because no 3-D Secure authentication is used by the merchant. If the merchant did not apply an acquirer exemption, the issuer should try to apply an issuer exemption or exclusion (MOTO, acquirer outside of EEA, MIT) where possible or soft decline the transaction (reason code 65).

NOTE: Issuers are exempted from this requirement where it may have a statutory obligation to do so.

Requirement 125: The issuer ACS should be capable of handling authentication requests from merchants in 3-D Secure 1.0 format or EMV 3-D Secure.

Merchants should bear in mind that the usage of EMV 3-D Secure ensures their compliance to the PSD2 RTS along with better performance and cardholder experience. Acquirers and issuers under PSD2 require transaction monitoring. It requires amongst others the validation of the authentication elements including devices, which only EMV 3-D Secure can transport but not 3-D Secure 1.0.

Acquirer Strong Consumer Authentication (SCA) Exemption

Below are the EUR specific requirements and recommendations, or both, around Acquirer Strong Cardholder Authentication (SCA) Exemptions.

NOTE: For more information on this topic, refer to **Additional Features** section of this document.

Mastercard proposes three options for Merchants and Acquirers to provide the required information to the Issuer when requesting SCA exemptions.

Option	Option Description	Option Benefits
1	EMV 3DS Authentication transaction with value '05' = No challenge requested; in SCA Exemptions field of the Merchant Data message extension (version 2.1) or '05' in 3DS Requestor Challenge Indicator (version 2.2), followed by Authorization	<p>The ARes in this option will return a Transaction status of "N" with reason code = 81 (version 2.1) or a Transaction status of "I" (version 2.2).</p> <p>The highly recommended option 1 will drive the highest authorization approval rate as a full EMV 3DS authentication request with all required data will be provided to the Issuer for an optimal "decisioning" process.</p>
2	Mastercard "Identity Check Insights" Authentication transaction (message category = 80) followed by Authorization	<p>For Mastercard Identity Check Insights, the ARes will return a Transaction Status of "U" (Authentication/ Account Verification Could Not Be Performed; Technical or other problem, as indicated in ARes or RReq) with a Transaction Status Reason Code = "80".</p> <p>The option 2 is an intermediate option allowing the Merchant to provide additional data but without going through the authentication process. The Issuer will receive cardholder and device insights in the authorization message. The anticipated approval rate of those transactions will be lower than fully authenticated transaction (option 1) but higher than no-EMV 3DS (option 3).</p>
3	No EMV 3DS Authentication. Straight to Authorization	This is the least preferred option as anticipated approval rate is the lowest.

The value "05 = No challenge requested (transactional risk analysis is already performed)" can be used for low-value payment (LVP), transactional risk analysis (TRA), recurring payment with fixed amount and Merchant-Initiated Transactions (MIT) Acquirer exemptions.

For European rules for acquirers and issuers regarding SCA exemptions, refer to announcement *AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions*.

Low-Value Payments and Management of Counters

According to the Second Payment Services Directive (PSD2) Regulatory Technical Standards on Strong Cardholder Authentication (SCA) and Secure Open Standards of Communication (RTS), payments are considered as low value if less than or equal to 30 euros or equivalent in other currencies.

The PSD2 RTS also set maximum above which Strong Cardholder Authentication (SCA) will be required

- Maximum number of consecutive transactions without SCA = 5
- Maximum cumulative amount of consecutive transactions without SCA = 100 euros or equivalent in other currencies.

The Low-Value Payments (LVP) exemption can be applied by issuers but as well by acquirers.

Because acquirers may not be able to count the number of all transactions and cumulative amount since the last SCA on a PAN, this must be done by the issuer. Issuer can do so by either managing the LVP counters at a token level (for example, on the payment device) or by leveraging the issuer authorization host system during authorization processing when acquirers apply the LVP SCA exemption. When these counters or cumulative amount limits are exceeded, issuers must respond with response code 65 (“Soft Decline”) and merchants must send an authentication request requesting a challenge.

A LVP exemption will be indicated by the merchant or acquirer using the 3DS Requestor Challenge Indicator = “05” in authentication and DE48 SE22 SF1 = “04” in authorization.

Merchant Fraud Rate

Merchant fraud rate is a data point provided by the merchant to the ACS/Issuer to increase its level of confidence in the ongoing transaction. Issuers may also use it to decide if a Merchant should be eligible for the white listing exemption.

NOTE: Refer to “Merchant Fraud Rate” under the “Additional Features” section of Chapter 2 for more details.

For European requirements on Merchant Fraud Rate, refer to the *Authentication Express Program Guide*.

Acquirer Country Code

If the transactions are “two-leg”, that is, acquirer’s and the issuer’s ISO country code is in the EEA, then related transactions are in scope of the PSD2 RTS on SCA.

NOTE: Refer to “Acquirer Country Code” under the “Additional Features” section of Chapter 2 for more details.

Thus, it is important to share the acquirer country code; otherwise, an ACS/Issuer could wrongly flag an ongoing transaction as a “one-leg” transaction, which would be out of scope of the PSD2 RTS on SCA.

For details on rules around Acquirer Country Code, refer to announcement *AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions*.

Recommendation: Even if the merchant country code matches the acquirer country code, it is still recommended to provide the acquirer country code in the Mastercard “Merchant Data” Message Extension.

Secure Corporate Payments Exemptions

In order for merchants to identify and indicate transactions for “secure corporate payments”, and where SCA exemption is desired, Mastercard has defined a message extension with a Secure Corporate Payment flag or field.

This allows merchants to indicate that dedicated processes and protocols were used as required for secure corporate payment exemption, by which the issuer’s ACS could then decide if indeed the transaction is eligible to apply the exemption.

For Europe for details on Secure Corporate Payments, refer to the *Authentication Guide*.

The table below details how secure corporate payment exemption will work.

NOTE: This works the same way for version 2.1 and 2.2.

Table 14: Feature: Secure Corporate Payment Exemption

3DS Version	Network	Description	
		Data Element	Values
2.1 & 2.2	Authentication	Message Flow	AReq = O
		Message Category	01- PA
		Device Channel	01- App, 02- Browser, and 03– 3RI
		Request Message (AReq)	
		“Merchant Data” Message Extension field “secureCorporatePayment”	Y
		3DS Requestor Challenge Indicator	02 (No challenge requested)

3DS Version	Network	Description	
		Data Element	Values
		<p>NOTE: For details on Merchant Data Message Extension refer to Appendix D - Merchant Data Message Extension.</p>	
		<p>Response Message (ARes or RReq)</p>	
		Transaction Status	Y
		ECI	02
		AAV leading Indicator	kA
		<p>NOTE: Response to a unauthenticated exemption request will be business as usual.</p>	
		<p>NOTE: For details around transaction processing refer to the Processing Matrix in Chapter 4.</p>	
	Authorization	<p>Successfully authenticated Secure Corporate Payment Exemption transactions are submitted in Authorization with the below.</p>	
		SLI	212
		DE48 SE22	SF1 = "06" in authorization to indicate Secure corporate payment
		<p>NOTE: Liability for this transaction is with the issuer.</p>	

For details on European rules around Secure Corporate Payments, refer to announcement *AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions*.

A Secure Corporate Payment Exemption can also be requested by the merchant straight in authorization by using DE48 SE22 SF1 = "06".

Merchant Whitelisting

'Whitelisting' of merchants exempts from applying SCA for any amount, regardless of the merchant's, acquirer's, and issuer's fraud rate; it enables and protects one-click payments

for cardholders, including card-on-file payment, as well as to enable recurring payments for variable amounts.

White listing enables a strong user experience and hence may reduce cardholder abandonment.

NOTE: For more information on Merchant Whitelisting, refer to Additional Features section of this document.

PSD2 has some very specific requirements for Merchant Whitelisting. For more details, refer to PSD2 Article 13.

NOTE: For recommended best practices on cardholder user experience for adding merchants and for managing the merchant white list, risk considerations and operational considerations, refer to the *Mastercard Standards for Merchant White Listing*.

Recurring Payments/MITs

EUR specific requirements and recommendations around recurring payments are below.

NOTE: Refer to the section on “recurring payments” in Chapter 3 of this guide for general information on how recurring transactions will work.

According to the Article 14 in EEA, a Strong Consumer Authentication (SCA) is required for the first transaction of the recurring payments. For details on enforcement dates, refer to announcement *AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions*.

Requirement 133: The SCA request for the first transaction must be indicated using the 3DS Requestor Challenge Indicator (Field Name: threeDSRequestorChallengeInd) field containing the value of 04 = Challenge requested (Mandate).

Requirement 134: In EEA, 3DS Requestor Prior Transaction data field must contain all nines (“9”) instead of DS Transaction ID for initial Recurring Payment authentication.

For European rules around 'grandfathering' of recurring payments and details on enforcement dates, refer to announcement *AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions*.

For European rules around the usage of 'Trace ID' in authorization for recurring payments, refer to announcement *AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions*.

Mastercard Services in Support of PSD2 RTS

Mastercard offers a variety of solutions or services to aid the EMV 3DS ecosystem and its stakeholders. Below are the services that are offered in support of PSD2 RTS.

Mastercard On-Behalf AAV Validation Service

For Europe for more details on how issuers can use the Mastercard On-Behalf AAV Validation Service perform the dynamic linking validation, refer to the *Authentication Guidelines*.

Authentication Express (Europe)

The PSD2 RTS requires that issuers perform Strong Cardholder Authentication (SCA) on remote e-commerce payment transaction. Issuers may choose to contract with other providers to conduct SCA on the issuers' behalf – delegate the SCA.

For more details, refer to Article 3, in the PSD2 RTS.

Authentication Express is Mastercard Europe's multilateral program that allows issuers to engage with authenticators (Device, Wallet or Merchant) to delegate SCA without the need for bilateral agreements.

For more information on the program and implementation requirements, refer to *Authentication Express Program Guide*.

Appendix A Mastercard Authentication Best Practices

This section describes the best practices when applying Mastercard Identity Check™ in the context of strong authentication.

Authentication Best Practices Introduction.....	130
Definition of Strong Authentication.....	130
Interpreting the Three Factors for Strong Authentication.....	131
Best Practices for Enhancing Consumer Experience.....	134
Authentication Methods not Allowed with Identity Check.....	137

Authentication Best Practices Introduction

Strong authentication for card not present transactions aims to reduce fraud in internet payments.

Alternatively, a risk-based approach to authentication can be used as long as this is effective in controlling fraud while providing an optimal consumer experience when authentication is required.

Not all authentication solutions are equal, and when reviewing them, an issuer should consider the consumer experience, the technical strength of the authentication, and its ability to prevent fraud. Friction at checkout has been proven to cause abandonment, and getting the correct balance is key to drive transaction volume.

The Mastercard Global Authentication strategy examines the balance between

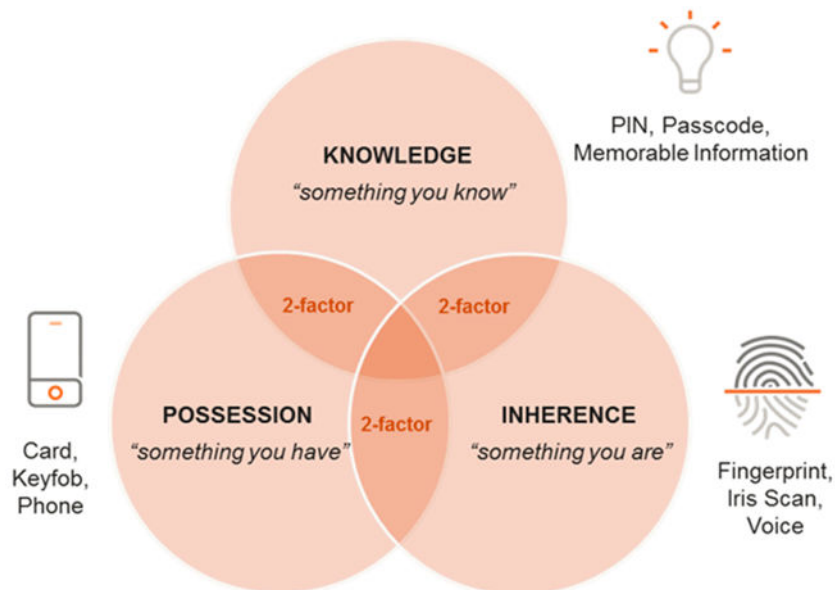
- Friction at checkout
- Fraud reduction for the industry
- A simple and good consumer experience
- An improved merchant experience for deployment of Mastercard authentication technologies

The remainder of this appendix describes best practices when applying Mastercard Identity Check™ in the context of strong authentication and consumer experience.

Definition of Strong Authentication

Strong authentication is defined as at least two of the following three factors.

1. Knowledge—something only the user knows. For example, a pass code or PIN.
2. Possession—something only the user possesses. For example, a mobile phone or token.
3. Inherence—something the user is; for example, a fingerprint, face, voice, or iris.



These factors chosen must also have the following characteristics

- Mutually independent—the breach of one does not compromise the reliability of the other.
- Non-reusable and non-replicable (except for inherence).
- Not capable of being stolen through the internet.

These conditions are difficult to meet in a world where information lives on the internet and can easily be replicated in e-commerce transactions.

Interpreting the Three Factors for Strong Authentication

The section below covers each of the three strong authentication factors that must be considered in detail.

Factor 1: Knowledge—Something Only the User Knows

A **something only the user knows** factor is something the consumer knows, such as a PIN, a passcode, or a special gesture applied on a touch screen.

When used, the consumer is aware it must be kept secret and no one except the consumer would know it (including the consumer's family and friends). In addition, **something you know** factors, when used, must permit at least 10,000 different possible responses that are equally probable.

Mastercard suggests a minimum length of six digits for any PIN. Mastercard also suggests that any PIN that is used for Internet sessions should be different from the PIN the consumer uses with their EMV[®] chip card where the PIN is exposed on the internet due to the sensitivity of this code.

A static password or a static PIN is a **something only the user knows** element.

A static password entered directly on a browser environment of the device used to initiate the transaction does not meet this requirement. When a static password is used, it must either be

- Entered on a separate device such as hand-held fob, or;
- Used to open an application that generates a one-time password, such as many legacy applications of Mastercard SecureCode™ (which, for example, then generates a one-time password).

In both cases, the dynamic password generated by the fob or the application (not the static password) is to be manually entered on the browser of the device where the transaction is initiated, or that the other strong authentication element used must meet the above requirements.

NOTE:

1. **Secret questions such as: your mother's maiden name, name of your first pet, make of your first car, are not secret (typically known by friends and family).**
2. **Card details such as last four digits of the PAN, card expiry date, cardholder's name, card billing address, and CVC2 are not considered secret for the purpose of this requirement.**

Existing use of Static Password with SecureCode is considered a single factor. Issuers that currently use this method of authentication are faced with decisions to make surrounding how to update their solution to become compliant with Mastercard Identity Check™.

Static Passwords Including Knowledge-Based Questions

The reasons for elimination of static passwords for Mastercard Identity Check include:

- Many, but not all, cardholders have a distaste of static passwords, especially those with more than one card account.
- There is a risk with any static data that it can become compromised through social engineering, key logging, phishing or vishing, and so on.
- A static password with another factor included can provide a complicated consumer experience.
- Existing static password solutions can be complex, especially those based on random characters from the static data.
- Most Static Password solutions include an automatic password reset capability that can allow account takeover and fraud if not carefully controlled.

Mastercard already prohibits the use of Static Passwords when an issuer chooses to deploy a risk-based solution to authentication. The benefit of the risk-based approach is to challenge a cardholder for a small number of transactions often as little as five to eight percent of the time. The reality is that using static password as a step-up authentication method is not just a very poor consumer experience; most cardholders will forget passwords that they don't frequently use, but also open the solution to fraud.

For the aforementioned reasons, Mastercard Identity Check Program requires a challenge that is not based on static data and a number of options exist today as detailed in this program guide.

Factor 2: Possession—Something Only the User Possesses

Something only you have factors must not be intended for being shared by multiple persons and may include multiple devices owned by a single person and must not be easily physically replicable.

Something you have factors are something the consumer possesses, such as a mobile device, a PC, a chip-card, a special purpose authentication device; for example, key fob. When used, must be intended for being used solely by an individual. **Something you have** factors that are often shareable by a small group of persons; for example, family desktop PCs, billing address, may also be used when the solution to check the factor used can reliably identify the specific person being authenticated.

Something only you have could cover multiple devices that the consumer possesses such as both a work and personal smart phone, personal PC and laptop device, or even work and home devices. A profile containing these devices that a consumer uses can both help predicting the user wishing to authenticate and in improving the consumer experience.

Something only you have factors, when consisting of a physical device, must be such that a person with commercially available technical means and reasonable technical knowledge is unable to replicate them at a reasonable cost. Likewise, **something only you have** factors must strongly protect against risk of a similar, but non-genuine, device achieving a positive authentication.

Factor 3: Inherence—Something the User is

Something you are is some biometrical characteristic of the consumer, such as a fingerprint, facial characteristics, voice, eye iris, heartbeat, etc. The method to identify **something you are** factors must strongly protect against risk of an inanimate replicas of the genuine consumer's biological factor achieving a positive authentication. These factors must be reasonable and unique to each person and protected from compromise. For example, when facial recognition is used, the solution must ensure that substituting a 2D picture for the real face of the consumer does not produce a valid authentication result by requiring that the consumer **blink** or perform some other **liveness** measure.

The factor must be such that chance that two different persons sharing the same biological characteristic being used by the factor should be low. In other words, the frequency of each instance of the biological characteristic should not be greater than 1 in 10,000.

NOTE: The frequency of identical twins seems to be around 1 in 250. Identical twins have different fingerprints.

The level of protection offered must be at least similar to a four-digit PIN.

Something you are factors must be deployed in a way to protect the biometric data within the device or network, and in a form that can allow the change of the token in the event of

compromise. This can be achieved in many ways including a store of an encrypted values based on various data points captured as part of the biometric scan. In this way, the value can be changed by changing the encryption key if there is concern of compromise, protecting the actual biometric characteristic of the user.

Best Practices for Enhancing Consumer Experience

The following best practices aim to improve the consumer experience to likely lead to a reduced abandonment rate.

- **Best Practice.** Provide solutions to support each customer segment's needs.
Best Practice Supported. When considering authentication, issuers should realize that no single solution will fit their customer segmentation approach and they may need differing solutions between, say, youth and silver surfer segments.
- **Best Practice.** Consider if strong authentication can meet the needs of all customer communication requiring security.
Best Practice Supported. There has been growth in the use of mobile and Internet Banking solutions in addition to the more traditional call center or telephone banking solutions offered for many years. This growth allows for a reconsideration of authentication needs between banks and their customers. Authentication of consumer using these services has been mixed and can be frustrating to the consumers. Added to this, issuers have struggled to balance the need for security questions that the cardholder can answer that the fraudster cannot.

Strong authentication suggests that a single solution could be identified that supports consumer authentication in all channels, versus separate solutions for each channel.

- **Best Practice.** Keep a profile of all devices that are being used by each consumer to reduce false risk alerts.
Best Practice Supported. Similarly, issuers must be able to handle and identify multiple devices for each consumer, such as multiple devices for online shopping and payment (such as, laptop and PC), as well as multiple devices for authentication (such as, mobile device with password/token generator, key fobs). Issuers are therefore recommended to manage a profile of these devices that a consumer uses as it can help to securely authenticate the user and to improve the consumer experience, especially if device data is gathered invisibly to the consumer.

It is also true that deploying a number of solutions, especially those that gather data that is invisible to the consumer, can increase the predictive nature, allowing a score to be developed that suggests confidence that the cardholder is genuine on any specific transaction. The next sections will address both geo-location and device data that can drive a risk based approach to authentication as well as other authentication methods that exist today.

- **Best Practice.** Incorporate geo-location as criteria into the authentication process.
Best Practice Supported. Given the move to an environment where the mobile phone will play a growing role in payments, the use of this device can be for more than just authentication. This can play an important role in determining if the phone, the user, the

purchase are all occurring in the same location and has already added value in the physical world. With geo-location tracking, it is possible to match the location of the cardholder's mobile with the locations of his or her transactions while traveling, reducing false-positive declines and removing some of the geo-blocking behavior we have seen in the past.

This same logic can still be added into a decision for remote payments when matched to device scanning/fingerprint, IP address and other characteristics supporting the option to undertake a risk based decision to authenticate or not.

- **Best Practice.** Use Risk-Based Authentication to reduce the cardholder abandonment rate.

Best Practice Supported. Both merchants and issuers can undertake a risk based approach to authentication (referred to as 'transaction risk analysis'), commonly known as Risk Based Authentication (RBA).

- With RBA, typically only 10 percent or less of transactions require a challenge to verify identity and experience shows that this does not increase fraud losses. This usually results in a significant reduction in the abandonment rate without an increase in fraud.

NOTE: These metrics are RBA program design targets and apply when the merchant is using RBA for a representative distribution of transactions. They cannot only authenticate the transactions that look risky and expect these metrics

- It is recommended that RBA evaluates each online transaction in real-time by measuring multiple fraud indicators to determine the risk level with statistical tools (typically self-learning) based on data such as:
 - Device parameters (including SIM ID/ICCD, device ID/IMEI, but also device 'fingerprints' such as IP address or WiFi MAC address, connection type, browser type or version, operating system and version, screen resolution and display size, language and time zone settings; or signs of malware infection)
 - Geo-location if available through the use of a mobile handset
 - Cardholder parameters (account number, transactional like time, location, amount or currency, velocity; but also changes such as name or language settings)
 - Merchant parameters (chargeback and fraud rate, merchant category, country)
- Among others, the following checks should be performed:
 - Is Cardholder account, device, or merchant on blacklist?
 - Monitor abnormal device, cardholder and merchant behavior patterns (such as a change of Internet Protocol (IP) address, different card used on device, high transaction amounts) and compare with known fraud patterns
 - Cookies are OK if they have the purpose of a smoother user experience. However, cookies should not be used to manage, facilitate or replace any process where SCA is required from the consumer at the time of transacting. Issuers must assess the risk of transactions where cookies are used, knowing that fraudsters can access them.
 - Was transaction initiated from a wallet?

- Use biometrics to improve consumer experience and to meet strong authentication requirements.
 - The use of biometric solutions can provide both a fantastic consumer experience and has the potential to fulfill all three categories of strong authentication dependent on how the solution is deployed. These applications can also alert the cardholder to a transaction being undertaken and allow them to cancel the transaction if it was not one that they intended to undertake. Use of the smart phone as a core part of authentication appears to provide opportunities for a segment of cardholders, even if solutions do not take advantage of biometrics but use the phone for other use cases such as to generate an OTP.
 - Enroll and activate cardholders before they conduct their first online payment to avoid abandonment.
 - A trusted environment is required to provision the strong authentication for the consumer, which means that the traditional Activation During Shopping (ADS), which often uses certain static questions, is not acceptable. Redirects are also known to cause increases in abandonment.
 - It is recommended that consumers are registered before they shop online, for example, when using online banking or at time of card issuance. The registration process should be safe and simple and should describe how the authentication process works and what to expect while shopping on-line at an enabled merchant.
- Monitor authentication process and contact cardholders after abandonment or inactivity to ensure card will be used successfully for the next online payment.
 - Consumers that abandon the authentication process during online shopping should be contacted afterward, such as through their online banking application or other trusted banking communication. They should be reminded about the authentication process with an option to ask questions (such as, to report a malfunction).
 - On screen, communication for a declined transaction is also recommended and should always list several key elements such as customer service number, website, and program name.
 - Issuers should explain their authentication programs on their website and include them as search term on their website. It should provide them with the expectations of their online check out experience with authentication techniques.
 - With OTP through SMS, when the authentication does not complete, it is recommended to send the cardholder another SMS or email asking to confirm the correctness of her mobile phone number. Without response, the issuer is recommended to contact the cardholder through other means to make sure that the latest mobile phone number is being used for authentication.
 - Consumers that have not used authentication or their cards online for a longer period (such as, six months) should be sent reminders about how their cards can be used online (including the authentication process).
- Avoid authentication methods requiring a device that the cardholder does not usually carry.
 - To ensure that consumers can shop online wherever they are, it is recommended to re-use items which consumers carry around (for example, mobile device,

payment card with display to show OTP) rather than providing a separate device (such as, Key Fob that displays OTP).

Authentication Methods not Allowed with Identity Check

The following provides examples of authentication methods that do not meet strong authentication requirements and provide the cardholder with challenging or poor consumer experiences and are no longer allowed with Mastercard Identity Check™.

Authentication method	Reason why it does not meet the Strong Authentication requirements
Password or PIN (when used as the only factor)	Only includes one factor (a something you know – the password). In addition, this is a type of factor that does not offer a strong level of protection against illicit replication and use.
Answer to a 'secret question'	Only includes one factor (a something you know – the password). In addition, this is a type of factor that does not offer a strong level of protection against illicit replication and use.
'Bingo Card' or list with codes (distributed by the issuer or by an ATM) whereby a different code is used for each authentication	Only includes one factor (a something you have – the card or list).
Variable static password (from which different characters are used for each authentication)	Only includes one factor (a something you know – the password).
Card reader not requiring a PIN	Only includes one factor (a something you have – the plastic card).
Interactive Card displaying a one-time code without requiring a PIN	Only includes one factor (a something you have – the plastic card).
Card displaying a dynamic CVC without requiring a PIN	Only includes one factor (a something you have – the plastic card).
Key Fob 'Digipass' that generates a one-time code without requiring a PIN	Only includes one factor (a something you have – the key fob).
Interactive Voice Response Systems that ask questions	Only includes one type of factor (something you know).
Knowledge Based Questions	Only includes one type of factor (something you know).

Appendix B Branding Guidelines

The section describes guidelines when using the Mastercard® brand.

Mastercard Identity Check Identifier.....	139
---	-----

Mastercard Identity Check Identifier

The Mastercard Identity Check™ Identifier must be used by participating issuers and merchants of the Identity Check Program.

Use is intended to signify participation in the program and thus must be displayed on websites. It may also be used in print and internet marketing collateral.

Use the Mastercard Brand Center hyperlink in Chapter 1, Contact Information section to access the guidelines and approved artwork.

Refer to **Requirement 90** for branding requirement in situations where the graphic logo or special characters cannot be used.

Appendix C Digital Transaction Insights

The Risk Level and Reason Codes that are part of Digital Transaction Insights (DTIs) are derived from the proprietary Mastercard proprietary Smart Authentication (RBA) platform.

Risk Levels 0-9.....	141
Reason Code Approach.....	141
Reason Codes.....	143

Risk Levels 0-9

The risk level is an assessment with values between 0-9; with 0 signifying the lowest risk and 9 signifying the highest risk. Risk levels are derived from the Mastercard Smart Authentication model.

The Mastercard Smart Authentication platform is designed to leverage all historical data available to Mastercard from the authentication and authorization (authorizations, debit, clearing, chargeback, SAFE, and so forth) processes. No external third party data is included in the model.

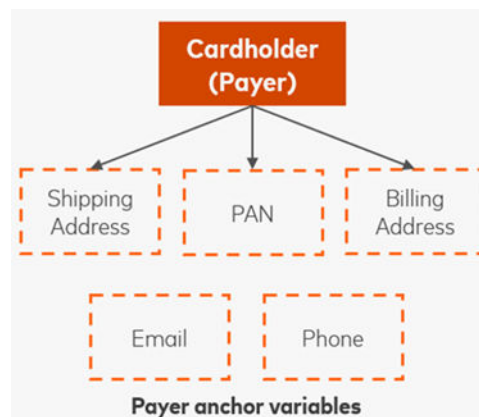
The Smart Authentication platform leverages

- **Short-term PAN** velocities and ratios (short term = minutes, hours, days, and weeks) in Authorization and Authentication: Measuring consistency and changes in behavior, for example, frequency, amount spent, declines, risk history, and so forth.
- **Long-term PAN** variables and ratios (Long term = one or more months, one or more years).

Reason Code Approach

Reason codes are built using a hierarchical approach.

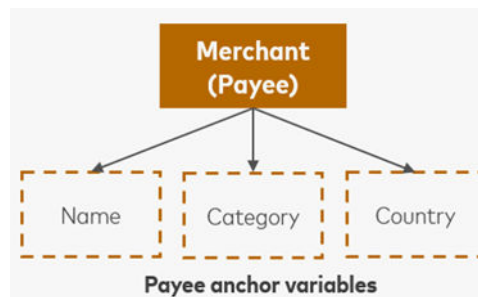
This approach starts by classifying the model variables into different entities, such as, cardholder (payer), merchant (payee), environment, and their respective anchor points; ultimately creating a hierarchical reason code that is based on which anchors, entities, and corresponding rules that are activated.



Anchor variables associated with the cardholder in the context of the given transaction and cardholder history

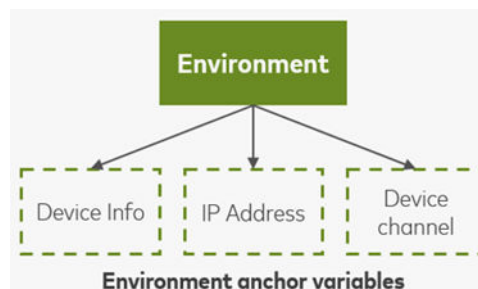
- Shipping address has been used with the primary account number (PAN) in the past N transactions

- Shipping address is unchanged from prior transaction
- PAN has had successful authentications in the past N transaction



Anchor variables associated with the merchant:

- Includes analyzing fraud rates, decline rates, non-cleared transaction rates, and so forth, at either the merchant or acquirer, or both.
- Merchant category and location is consistent with other transactions from the merchant in the past



Anchor variables associated with device and the current authentication session:

- Internet Protocol (IP) address is known and not a Bad IP
- Device is known and not a Bad device
- Device has had successful authentications in the past N transactions

NOTE: The above is not an exhaustive list of anchors.

Reason codes are loosely structured in a hierarchical order driven by data connections.

- **Strong:** if a certain anchor variable within a category, for example, cardholder (payer) is established and known based on historical transaction data – a positive reason code related to that anchor is issued.
- **Stronger:** if there is a connection between categories, for example, cardholder (payer) and device (environment) – this is a stronger positive indicator and a suitable reason code related to both categories is issued.
- **Strongest:** if there is a connection between all three categories, for example, cardholder (payer) and device (environment) and merchant (payee) this is the most positive strong signal.

Examples of potential positive signals with anchors and variable categories.

1. One cardholder (payer) anchor established, for example, shipping address is consistent:
 - Shipping address has been used with the PAN in the past N transactions
 - Shipping address is same as billing address on file
 - Shipping address is not on a blacklist
 - Shipping address is unchanged from prior transaction
2. More than one cardholder (payer) anchor established, for example, multiple cardholder anchors consistent:
 - Shipping address is consistent
 - Billing address is consistent
 - PAN has historical positive association with cardholder
 - Purchase amount, date, and time is consistent
3. Co-occurring cardholder (payer) and merchant (payee) link established, for example, cardholder shows consistent activity and has established history at the merchant.
 - Contact information consistent for cardholder
 - Trusted cardholder and transaction
 - Trusted merchant
 - PAN shows established activity and authentication history at the given merchant
4. Potential reason codes arranged roughly in order from negative to positive (from risk events to highly trusted).

Reason Codes

The reader can use this section to interpret the Reason Codes provided as part of the DTI assessment.

Code	Reason Code Name	Description and Comments
A	Risk Event - Suspicious Account Activity	Mastercard has detected suspicious activity with cardholder's account.
B	Risk Event - Unknown Device/ Account Relationship	Mastercard has not established a relationship between the device and account.
C	Risk Event - Device or Profile Information associated with fraud event	The device used for the transaction or the user's profile has been associated with a fraud event.
D	Risk Event - Recent High Risk Change to Device or Profile Information	The device used for the transaction or the user's profile has recently had a high risk change.

Code	Reason Code Name	Description and Comments
E	Risk Event - Recent change to Device or Profile Information	The device used for the transaction or the user's profile has recently changed.
F	Risk Event - PAN associated with fraud event	Mastercard has detected fraud associated with the PAN used for this transaction.
G	New Account or Insufficient Data	Cardholder details are new to Mastercard or there is insufficient data for this cardholder.
H	Merchant/ Acquirer: Merchant (fraud) risk high (assessed by Mastercard)	Mastercard has determined that the merchant is submitting transactions with a high rate of fraud.
I	Merchant/ Acquirer: Merchant (fraud) risk low (assessed by Mastercard)	Mastercard has determined that the merchant is submitting transactions with a higher rate of fraud than average.
J	Environment: Good/ Known IP	Mastercard is familiar with the IP where the transaction is happening and has assessed that it is a trusted IP.
K	Cardholder: Billing address – prior history established	Mastercard has established a positive association between the cardholder and this billing address.
L	Cardholder: Email address – prior history established	Mastercard has established a positive association between the cardholder and this email address. NOTE: Email address is an Identity Check optional field.
M	Cardholder: Phone number – prior history established	Mastercard has established a positive association between the cardholder and this phone number. NOTE: Phone number is an Identity Check optional field.

Code	Reason Code Name	Description and Comments
N	Cardholder: Shipping address – prior history established	Mastercard has established a positive association between the cardholder and this shipping address. Shipping address is an Identity Check required field for a transaction with a physical good.
O	Cardholder: Card number (PAN) behavior established high trust in the current transaction	Mastercard has established high trust in the transaction based on historical PAN behavior.
P	Environment: Device known	Mastercard has seen the device used for the transaction before, but this account might not be established on device.
Q	Environment: Account established on Device	Mastercard has seen this account transaction on this device and account has been authenticated on the device
R	Environment: Session - Trusted/normal/ innocent session (no man in the middle attack / no bot, not suspicious account activity)	This is about the quality of the session.
S	More than one Cardholder category established	Mastercard has established multiple Cardholder category anchors.
T	More than one Merchant/ Acquirer category established	Mastercard has established multiple merchant category anchors.
U	More than one Environment category established	Mastercard has established multiple Environment category anchors.
V	Co-occurring: established link between Cardholder and Merchant/ Acquirer	Mastercard has established linkages across Cardholder and merchant/ acquirer categories.
W	Co-occurring: established link between Cardholder and Environment	Mastercard has established linkages across Cardholder and Environment categories.
X	Co-occurring: established link between Merchant/Acquirer and Environment	Mastercard has established linkages across merchant/ acquirer and Environment categories.

Code	Reason Code Name	Description and Comments
Y	All three categories established	Mastercard has established linkages across Cardholder, merchant/acquirer and Environment categories.
Z	Most trusted	Reserved for Future Use.

The reason codes above are arranged roughly in order from negative to positive (from risk events to highly trusted).

NOTE: From the Mastercard perspective, the profile means the cardholder's primary account number, shipping address, device, and so forth.

Appendix D Merchant Data Message Extension

The merchant data message extension is used to pass information and data from the merchant to the ACS or issuer which is not supported by the EMV 3DS specification.

Merchant Data..... 148

Merchant Data

The below are the details for the Mastercard defined “Merchant Data” message extension.

```
"messageExtension": [{
  "name": "Merchant Data",
  "id": "A000000004-merchantData",
  "criticalityIndicator": false,
  "data": {
    "A000000004-merchantData": {
      "scaExemptions": "05",
      "merchantFraudRate": "1" ,
      "acquirerCountryCode": "050",
      "secureCorporatePayment": "Y"
    }
  }
}]
```

Table 15: “Merchant Data” message extension field validations:

Field	Field Name	Validations
1	scaExemptions	<p>Optional field (not required to be present in the message extension)</p> <p>Only allowed for version 2.1 of EMV 3DS. DS will remove/drop field from the message extension if present in version 2.2 of EMV 3DS message and continue processing</p> <p>Must be numeric</p> <p>Must have two bytes. The zero on the left must be present if it is a number below 10. The number five, for example, without the zero on the left must be considered an incorrect value</p> <p>Allowed values: 05, 06, 07</p>

Field	Field Name	Validations
2	merchantFraudRate	<p>Optional (not required to be present in the message extension).</p> <p>Allowed for both version 2.1 and 2.2 of EMV 3DS.</p> <p>Must be numeric</p> <p>Maximum length of 2 bytes</p> <p>Allowed Values:</p> <p>1 (represents fraud rate <=1)</p> <p>2 (represents fraud rate 1+ - 6)</p> <p>3 (represents fraud rate 6+ - 13)</p> <p>4 (represents fraud rate 13+ - 25)</p> <p>5 (represents fraud rate >25)</p>
3	acquirerCountryCode	<p>Optional (not required to be present in the message extension).</p> <p>Allowed for both version 2.1 and 2.2 of EMV 3DS.</p> <p>Must have three bytes. The zero on the left must be present if it is a number below 100. The number five, for example, without the zero on the left must be considered an incorrect value.</p> <p>Must be numeric.</p> <p>Allowed values: Any ISO country code.</p>

Field	Field Name	Validations
4	secureCorporatePayment	Optional (not required to be present in the message extension). Allowed for both version 2.1 and 2.2 of EMV 3DS. Maximum length of one byte. Must be alphabetic. Not case sensitive. Allowed values: Y, N.

Appendix E ACS Data Message Extension

The ACS data message extension is used to pass information/ data from the ACS/ issuer to the merchant which is not supported by the EMV 3DS specification.

ACS Data..... 152

ACS Data

The below are the details for the Mastercard defined “ACS Data” message extension.

```
These are the details for the Mastercard defined “ACS Data” message extension.
"messageExtension": [{
  "name": "ACS Data",
  "id": "A000000004-acsData",
  "criticalityIndicator": false,
  "data": {
    "A000000004-acsData": {
      "whitelistStatus": "Y"
    }
  }
}]
```


Table 16: “ACS Data” message extension field validations:

Field	Field Name	Validations
1	whitelistStatus	<p>Optional (not required to be present in the message extension).</p> <p>Only allowed for version 2.1 of EMV 3DS. DS will remove or drop field from the message extension if present in version 2.2 of EMV 3DS message and continue processing.</p> <p>Maximum length of 1 byte</p> <p>Must be alphabetic</p> <p>Not case sensitive</p> <p>Allowed values:</p> <p>Y (represents 3DS Requestor is whitelisted by cardholder)</p> <p>N (represents 3DS Requestor is not whitelisted by cardholder)</p> <p>E (represents Not eligible as determined by issuer)</p> <p>P (represents Pending confirmation by cardholder)</p> <p>R (represents Cardholder rejected)</p> <p>U (represents Whitelist status unknown, unavailable, or does not apply)</p>

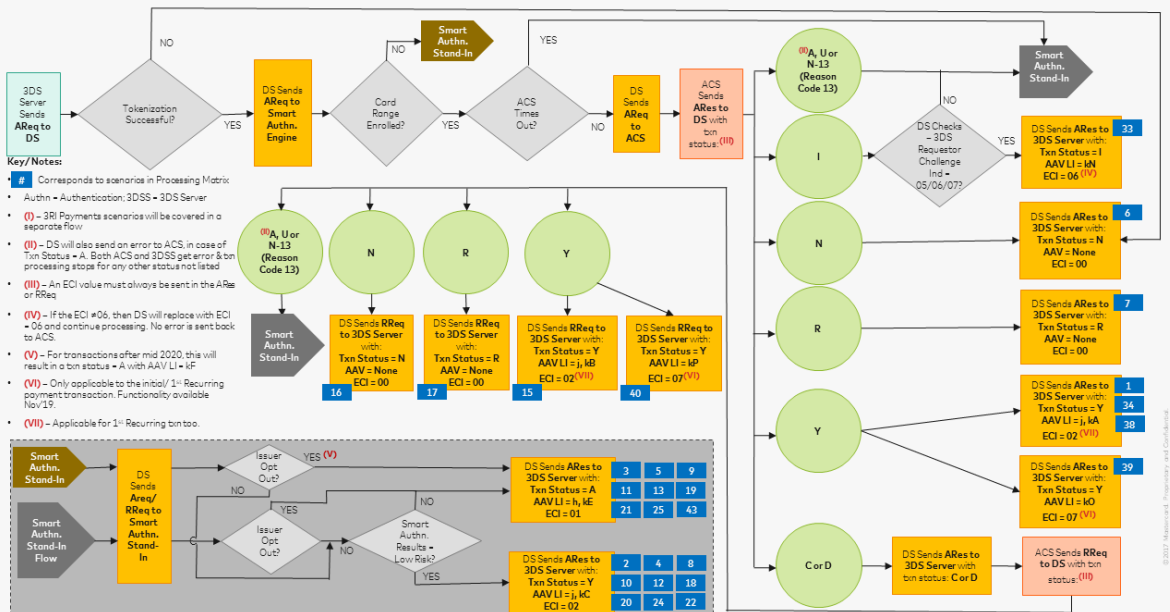
Appendix F Payment Transaction Flow (Version 2.1 and 2.2)

The Payment Transaction flow for versions 2.1 and 2.2 of EMV 3DS is documented in this topic.

Payment Transaction Flow (Both Versions) 155

Appendix F - Payment Transaction - Authentication Flow (Version 2.2)

Message Category =01 (PA)
Device Channel=01 (App) or 02 (Browser)



Appendix G Non-Payment Transaction Flow (Version 2.1 and 2.2)

The Non-Payment Transaction flow for versions 2.1 and 2.2 of EMV 3DS is documented in this topic.

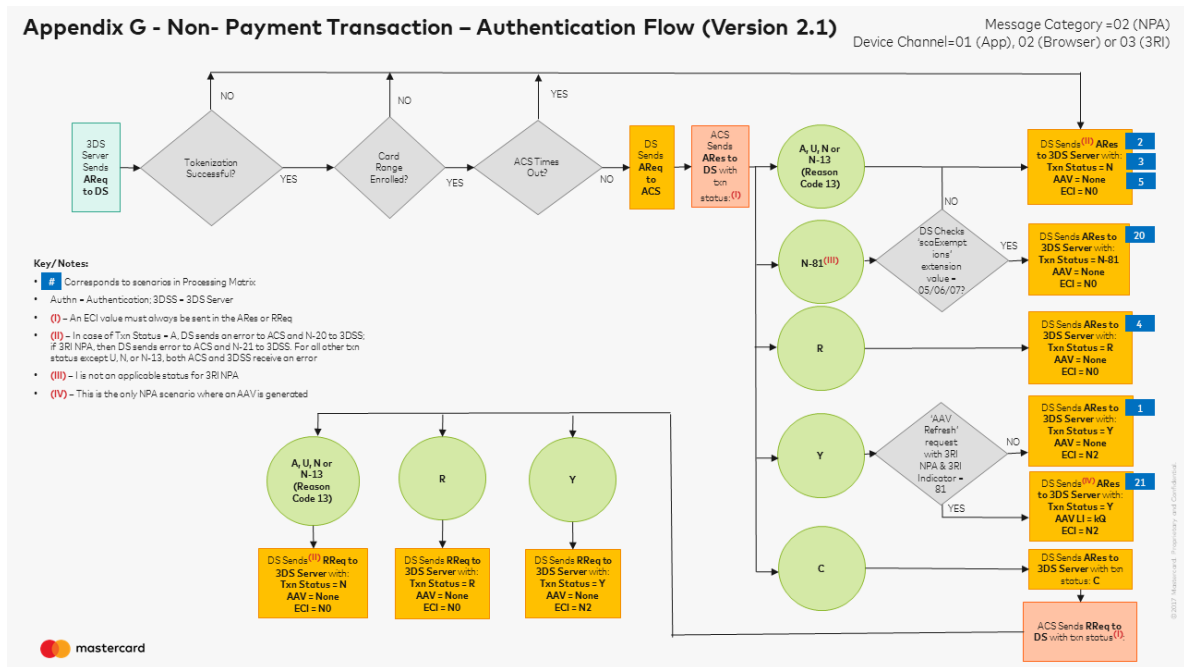
Non-Payment Transaction Flow (Both Versions)	158
--	-----

Non-Payment Transaction Flow (Both Versions)

Below is the Non-Payment Transaction flow for EMV™ 3DS.

Version 2.1

Below is the Non-Payment Transaction flow for Version 2.1 of EMV 3DS



Version 2.2

Below is the Non-Payment Transaction flow for Version 2.2 of EMV 3DS

Appendix H BIN Table Resource

This topic describes what is the BIN Table Resource and its benefits.

BIN Table Resource..... 161

BIN Table Resource

The BIN Table Resource provides a list of active and valid issuing account ranges to help Merchants and service providers successfully accept Mastercard transactions and prevent valid accounts from being declined.

Value-add to Merchants

Reliability	Accurate lists are provided directly by Mastercard – the most reliable source for up-to-date information.
Efficiency	With direct access to information, there is no need to continually monitor unauthorized lists.
Insight	Helps improve routing, fraud “decisioning”, information on brand, product and authorization.

BIN Table Resource provides authorization parameters ensuring greater BIN information accuracy.

- Authorization Only—identifies accounts from which a private label or prepaid card has been issued to provide Cardholder with prefunded discount or prepaid value only redeemed at select Merchants at checkout;
- Issuing Country Code—assists in e-commerce fraud management to help detect inconsistencies between the IP address of the originating purchase and the Cardholder billing address that may warrant additional analysis.
- Local Use—identifies whether cards within the authorization account range may be used outside of the country of issuance;
- Brand Product Code—identifies the Mastercard accepted brands: Mastercard Credit, Mastercard Debit, Maestro®, Cirrus®, and Mastercard Private Label;
- Series 2 BINs—range of BINs that begin with “2” and are processed the same as the series “5” BINS.
- The BIN table resources is a product which requires a service agreement. Information on the BIN table resource can be found on the Mastercard Developer Zone at this URL: <https://developer.mastercard.com/product/bin-table-resource>.

Appendix I Identity Check Insights – Sample Responses

A response message is returned from 3D Secure Server to 3D Secure merchant (sample successful and failure responses are below).

Identity Check Insights – Sample Success Responses	163
Identity Check Insights – Sample Failed Response	163

Identity Check Insights – Sample Success Responses

A response message is returned from 3D Secure Server to 3D Secure merchant (successful sample responses are below).

A response message (ARes) should be returned by 3D Secure Server to the requestor with “transStatus” field = “U”, transStatusReason=”80”, “threeDSServerTransID” and “dsTransID” should be populated. There will be ECI in the response November, 2019.

```
{
  "messageVersion": "2.1.0",
  "messageType": "ARes",
  "acsTransID": "3321de0d-0549-412a-9e1e-455a76a59053",
  "acsReferenceNumber": "EMVCoTrackUpto32EMVCoTrackUpto32",
  "dsReferenceNumber": "EMVCoTrackUpto32EMVCoTrackUpto32",
  "dsTransID": "3321de0d-0549-412a-9e1e-455a76a59053",
  "threeDSServerTransID": "0ea20865-b0df-44d1-9fda-10e6d07fc996",
  "transStatusReason": "80",
  "transStatus": "U",
  "sdkTransID": "d12345e0-67f3-23e5-a151-feff891cdc9f",
}
```

This response will also contains the ECI= 04. Here is what it would look like:

```
{
  "messageVersion": "2.1.0",
  "messageType": "ARes",
  "acsTransID": "3321de0d-0549-412a-9e1e-455a76a59053",
  "acsReferenceNumber": "EMVCoTrackUpto32EMVCoTrackUpto32",
  "dsReferenceNumber": "EMVCoTrackUpto32EMVCoTrackUpto32",
  "dsTransID": "3321de0d-0549-412a-9e1e-455a76a59053",
  "threeDSServerTransID": "0ea20865-b0df-44d1-9fda-10e6d07fc996",
  "transStatusReason": "80",
  "transStatus": "U",
  "sdkTransID": "d12345e0-67f3-23e5-a151-feff891cdc9f",
  "eci": "04"
}
```

Identity Check Insights – Sample Failed Response

A response message is returned from 3D Secure Server to 3D Secure merchant (sample failed response is below).

A failed Identity Check Insights transaction will have a response message (Ares) containing an extension called the “MAIQ response” (in bold below) with a status of fail to indicate an unsuccessful Identity Check Insights transaction.

```
{
  "messageVersion": "2.1.0",
  "messageType": "ARes",
  "messageExtension": [ {
    "name": "MAIQ response",
    "id": "A000000004-maiqRes",
    "criticalityIndicator": false,
  }
]
```

```
    "data": {"A000000004-maiqRes": {"status": "fail"}}
  ]],
  "acsTransID": "ae474c45-eea5-4902-98d4-3364e9dbaebf",
  "acsReferenceNumber": "EMVCoTrackUpto32EMVCoTrackUpto32",
  "dsReferenceNumber": "EMVCoTrackUpto32EMVCoTrackUpto32",
  "dsTransID": "ae474c45-eea5-4902-98d4-3364e9dbaebf",
  "threeDSServerTransID": "00060000-94f1-4583-8ea4-c4970b1b4409",
  "transStatusReason": "80",
  "transStatus": "U",
  "sdkTransID": "d12345e0-67f3-23e5-a151-feff891cdc9f"
}
```

Appendix J Regular E-commerce Payment Transaction— Authorization Data Elements

The ACS data message extension is used to pass information or data from the ACS/issuer to the merchant which is not supported by the EMV 3DS spec.

Authorization Data Elements.....	166
----------------------------------	-----

Authorization Data Elements

The table below lists some of the key fields that are recommended by the Identity Check Program to be populated in the authorization message for a regular e-commerce payment transaction.

Any fields that are required by the program are covered in Chapters 3, 4, and 5 of this guide. Additional transaction processing rules may apply based on the issuer and acquirer unique processing needs. It is recommended that issuers and acquirers use the processing logic that best applies to their transaction processing needs and scenarios.

NOTE: The *Authorization Customer Interface Specification (CIS)* manual is always the most up to date source for information on all authorization fields. The table below is based on the CIS manual published 9 April 2019.

NOTE: For the “inclusion” column of the table R= Required, O= Optional, C= Conditional.

Authentication Source	Data Elements	Inclusion	Single Charge (Regular e-commerce Payment)
	DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	R	00 (Purchase)
purchaseAmount	DE 4 (Amount, Transaction)	R	Purchase Amount
	DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	R	81 = PAN entry via electronic commerce, including chip or 10 = Credential on File

	DE 48 (Additional Data —Private Use), TCC (Transaction Category Code)	R	Contains one of the following values: P = Payment Transaction T = Phone, Mail, or e-commerce Order U = Unique X = Airline and Other Transportation Services (irrespective of the transaction origin is face to face or not)
3DS Requestor Authentication Indicator = 02 or 3DS Requestor Challenge Indicator = 05 or 07 (2.2 and greater) SCA Exemption Field 1 (2.1 only) = 05 or 07	48, subelement 22, subfield 01 (Low Risk Merchant indicator)	C*	*Required only for EUROPE if mentioned authentication fields were used. Optional for rest of the world 01 = Merchant Initiated Transaction 02 = Acquirer Low-Fraud and Transaction Risk Analysis 03 = Recurring Payment 04 = Low-Value Payment 05 = Strong Customer Authentication (SCA) Delegation
Electronic Commerce Security Level Indicator (SLI) from ARes	DE 48, subelement 42 (Electronic Commerce Security Level Indicator)	R	Contains security level in positions 1 and 2 and UCAF collection indicator in position 3. Position 1 (Security Protocol) = 2 (Channel) Position 2 (Cardholder Authentication) = 1 (e-commerce / SecureCode) Position 3 (UCAF Collection Indicator) = ECI from ARES

Authentication Value (AAV) from ARES	DE 48, subelement 43 (Universal Cardholder Authentication) for Mastercard SecureCode issuer or cardholder generated authentication data	C – required for all transaction statuses except N, R and C	Authentication Value (AAV) from ARES
	DE 48, subelement 63 (Trace Id)	C	Not Applicable
	DE 48, subelement 66 (Authentication Data), subfield 1 (Program Protocol)	R	1 = 3-D Secure Version 1.0 (3DS 1.0) 2 = EMV 3-D Secure (3DS 2.0)
DS Transaction ID from ARES	DE 48, subelement 66 (Authentication Data), subfield 2 (Directory Server Transaction ID)	R	Value from ARES Note: Only for EMV 3DS 2.0 transactions, DE 48 SE 66 SF 1 = 2
	DE 48 (Additional Data —Private Use), subelement 82 (Address Verification Service Request)	O	Not Applicable
	DE 48, subelement 92 (CVC 2 Value)	O	
	DE 61 (Point-of-Service (POS) Data), subfield 1 (POS Terminal Location)	R	1 = Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA) 2 = No terminal used (voice/audio response unit [ARU] authorization); server
	DE 61 Subfield 2- Reserved for Future Use	R	0 Reserved for Future Use

DE 61 (Point-of-Service (POS) Data), subfield 3 (POS Terminal Location)	R	2 = Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA) 3 = No terminal used (voice/ARU authorization); server
DE 61, subfield 4 (POS Cardholder Presence)	R	5 = Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA])
DE 61, subfield 5 (POS Card Presence)	R	1 = Card not present
DE 61 Subfield 6 - POS Card Capture Capabilities	R	0 = Terminal/operator does not have card capture capability
DE 61, subfield 7 (POS Transaction Status)	R	0 = Normal request (original presentment) NOTE: An e-commerce transaction may be submitted as either a preauthorization (DE 61, subfield 7 value 4) or final authorization (DE 61, subfield 7, value 0 and DE 48, subelement 61, subfield 5, value 1) by card acceptors in the Europe region.
DE 61 Subfield 8- POS Transaction Security	R	0 = No security concern 1 = Suspected fraud (merchant suspicious—code 10) 2 = ID verified
DE 61 Subfield 9- Reserved for Future Use	R	0 Reserved for Future Use

DE 61 Subfield 10 - Cardholder-activated Terminal level	R	6 = Authorized Level 6 CAT: Electronic commerce
DE 61 Subfield 11 - POS Card Data Terminal Input Capability Indicator	R	0 = Input capability unknown or unspecified. 1 = No terminal used (voice/ARU authorization); server. 6 = Terminal supports key entry input only.
DE 61 Subfield 12 - POS Authorization Life Cycle	R	Indicates the number of days the preauthorization stays in effect; ATM and Maestro POS transactions should use 01, Visa CPS transactions use applicable value. Must be zero filled when not applicable.
DE 61 Subfield 13 - POS Country Code (or Sub-Merchant Information, if applicable)	R	ISO Country Code
DE 61 Subfield 14 - POS Postal Code	R	Postal code of merchant location. Must not be blank filled.

Appendix K Recurring Payment Transaction—Authorization Data Elements

This topic contains details of the Recurring Payment Transaction—Authorization Data Elements.

Authorization Data Elements	172
-----------------------------------	-----

Authorization Data Elements

The table below lists some of the key fields that need to be populated in the authorization message for a recurring payment transaction.

There are two distinct columns in this table to highlight the differences between authorization messages for the initial or first recurring payment transaction versus the subsequent recurring payment transactions.

Any fields that are required by the program are covered in Chapters 3, 4, and 5 of this guide. Additional transaction processing rules may apply based on the issuer and acquirer unique processing needs. It is recommended that issuers and acquirers use the processing logic that best applies to their transaction processing needs and scenarios.

NOTE: The *Authorization Customer Interface Specification (CIS)* manual is always the most up to date source for information on all authorization fields. The table below is based on the CIS manual published 9 April 2019. For the “inclusion” column of the table below R= Required, O= Optional, C= Conditional.

Authentication Source	Data Element	Inclusion	Initial Recurring	Subsequent Recurring
	DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code)	R	00 (Purchase)	00 (Purchase)
purchaseAmount	DE 4 (Amount, Transaction)	R	Purchase Amount	Purchase Amount
	DE 22 (Point-of-Service (POS) Entry Mode), subfield 1 (POS Terminal PAN Entry Mode)	R	81 = PAN entry via e-commerce, including chip or 10 = Credential on File	10 = Credential on File

Authentication Source	Data Element	Inclusion	Initial Recurring	Subsequent Recurring
	DE 48 (Additional Data—Private Use), TCC (Transaction Category Code)	R	Contains one of the following values: P = Payment Transaction T = Phone, Mail, or Electronic Commerce Order U = Unique X = Airline and Other Transportation Services (irrespective of the transaction origin is face to face or not)	Contains one of the following values: P = Payment Transaction T = Phone, Mail, or Electronic Commerce Order U = Unique X = Airline and Other Transportation Services (irrespective of the transaction origin is face to face or not)
3DS Requestor Authentication Indicator = 02 or 3DS Requestor Challenge Indicator = 05 or 07 (2.2 and greater) SCA Exemption Field 1 (2.1 only) =05 or 07	48, subelement 22, subfield 01 (Low Risk Merchant indicator)	C*	*Not Applicable for Europe since SCA is mandated. Optional for rest of the world if mentioned authentication fields were used. 01 = Merchant Initiated Transaction 02 = Acquirer Low-Fraud and Transaction Risk Analysis 03 = Recurring Payment 04 = Low-Value Payment 05 = Strong Customer Authentication (SCA) Delegation	*Required only for EUROPE. Optional for rest of the world if mentioned authentication fields were used. 03 = Recurring Payment

Authentication Source	Data Element	Inclusion	Initial Recurring	Subsequent Recurring
Electronic Commerce Security Indicator (SLI) from ARes	DE 48, subelement 42 (Electronic Commerce Security Level Indicator)	R	Contains security level in positions 1 and 2 and UCAF collection indicator in position 3. Position 1 (Security Protocol) = 2 (Channel) Position 2 (Cardholder Authentication) = 1 (e-commerce / SecureCode) Position 3 (UCAF Collection Indicator) = ECI from ARES	Contains security level in positions 1 and 2 and UCAF collection indicator in position 3. Position 1 (Security Protocol) = 2 (Channel) Position 2 (Cardholder Authentication) = 1 (e-commerce / SecureCode) Position 3 (UCAF Collection Indicator) = ECI from ARES
Authentication Value (AAV) from ARES	DE 48, subelement 43 (Universal Cardholder Authentication) for Mastercard SecureCode issuer or cardholder generated authentication data.	C – required for all transaction statuses except N, R and C	Authentication Value from ARES	Authentication Value from ARES
	DE 48, subelement 63 (Trace Id)	C	Not Applicable	Trace Id of Initial Transaction NOTE: Values are <ul style="list-style-type: none"> • Positions 1–3 = “MCC” • Positions 4–9 = “999999” • Positions 10–13 = 1231 • Positions 14–15 = blank filled

Authentication Source	Data Element	Inclusion	Initial Recurring	Subsequent Recurring
	DE 48, subelement 66 (Authentication Data), subfield 1 (Program Protocol)	R	1 = 3-D Secure Version 1.0 (3DS 1.0) 2 = EMV 3-D Secure (3DS 2.0)	1 = 3-D Secure Version 1.0 (3DS 1.0) 2 = EMV 3-D Secure (3DS 2.0)
DS Transaction ID from ARES	DE 48, subelement 66 (Authentication Data), subfield 2 (Directory Server Transaction ID)	R	Value from ARES NOTE: Only for EMV 3DS 2.0 transactions, DE 48 SE 66 SF 1 = 2	Value from ARES NOTE: Only for EMV 3DS 2.0 transactions, DE 48 SE 66 SF 1 = 2
	DE 48 (Additional Data—Private Use), subelement 82 (Address Verification Service Request)	O	Not Applicable	Not Applicable
	DE 48, subelement 92 (CVC 2 Value)	O		
	DE 61 (Point-of-Service (POS) Data), subfield 1 (POS Terminal Location)	R	1 = Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA) 2 = No terminal used (voice/audio response unit [ARU] authorization); server	1 = Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA) 2 = No terminal used (voice/audio response unit [ARU] authorization); server
	DE 61 Subfield 2- Reserved for Future Use	R	0 (Reserved for Future Use)	0 (Reserved for Future Use)

Authentication Source	Data Element	Inclusion	Initial Recurring	Subsequent Recurring
	DE 61 (Point-of-Service (POS) Data), subfield 3 (POS Terminal Location)	R	2 = Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA) 3 = No terminal used (voice/ARU authorization); server	2 = Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA) 3 = No terminal used (voice/ARU authorization); server
	DE 61, subfield 4 (POS Cardholder Presence)	R	4 = Standing order/recurring transactions 4 is the value that should be used for all subsequent recurring payments globally. NOTE: Value 4 allowed for the Europe Region as of 14 September 2019. 5 = Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA])	
	DE 61, subfield 5 (POS Card Presence)	R	1 = Card not present	1 = Card not present
	DE 61 Subfield 6 - POS Card Capture Capabilities	R	0 = Terminal/operator does not have card capture capability	0 = Terminal/operator does not have card capture capability

Authentication Source	Data Element	Inclusion	Initial Recurring	Subsequent Recurring
	DE 61, subfield 7 (POS Transaction Status)	R	0 = Normal request (original presentment) NOTE: An e-commerce transaction may be submitted as either a preauthorization (DE 61, subfield 7 value 4) or final authorization (DE 61, subfield 7, value 0 and DE 48, subelement 61, subfield 5, value 1) by card acceptors in the Europe region	0 = Normal request (original presentment) NOTE: An e-commerce transaction may be submitted as either a preauthorization (DE 61, subfield 7 value 4) or final authorization (DE 61, subfield 7, value 0 and DE 48, subelement 61, subfield 5, value 1) by card acceptors in the Europe region.
	DE 61 Subfield 8- POS Transaction Security	R	0 = No security concern 1 = Suspected fraud (merchant suspicious—code 10) 2 = ID verified	0 = No security concern 1 = Suspected fraud (merchant suspicious—code 10) 2 = ID verified
	DE 61 Subfield 9- Reserved for Future Use	R	0 = Reserved for Future Use	0 = Reserved for Future Use
	DE 61 Subfield 10 - Cardholder-activated Terminal level	R	6 = Authorized Level 6 CAT: Electronic commerce	0 = Not a CAT transaction 6 = Authorized Level 6 CAT: Electronic commerce

Authentication Source	Data Element	Inclusion	Initial Recurring	Subsequent Recurring
	DE 61 Subfield 11 - POS Card Data Terminal Input Capability Indicator	R	0 = Input capability unknown or unspecified. 1 = No terminal used (voice/ARU authorization); server. 6 = Terminal supports key entry input only.	6 = Terminal supports key entry input only.
	DE 61 Subfield 12 - POS Authorization Life Cycle	R	Indicates the number of days the preauthorization stays in effect; ATM and Maestro™ POS transactions should use 01, Visa CPS transactions use applicable value. Must be zero filled when not applicable.	Indicates the number of days the preauthorization stays in effect; ATM and Maestro POS transactions should use 01, Visa CPS transactions use applicable value. Must be zero filled when not applicable.
	DE 61 Subfield 13 - POS Country Code (or Sub-Merchant Information, if applicable)	R	ISO Country Code	ISO Country Code
	DE 61 Subfield 14 - POS Postal Code	R	Postal code of merchant location. Must not be blank filled.	Postal code of merchant location. Must not be blank filled.

Appendix L Transaction Status, SLI, and Liability Mapping

The table below maps various payment scenarios with their associated Transaction Status, ECI, SLI, SPA 2 AAV Leading Indicators and Transaction Liability.

Transaction Status.....	180
-------------------------	-----

Transaction Status

This topic details mapping of payment transaction status, ECI, SLI, SPA 2 AAV leading indicators and transaction liability.

Scenarios	Txn Status	SPA2 AAV Leading Indicator	ECI	SLI	Liability of Txn
		SHA256 Encryption			
Transaction successfully authenticated by ACS - Frictionless	Y	kA	02	212	Merchant gets liability shift
Transaction successfully authenticated by ACS - Challenge	Y	kB	02	212	Merchant gets liability shift
Transaction successfully authenticated by Mastercard Smart Authentication Stand-In - Frictionless (low risk)	Y	kC	02	212	Merchant gets liability shift
Transaction successfully authenticated by Mastercard Smart Authentication Stand-In - Frictionless (non-low risk)	A	kE	01	211	Merchant gets liability shift
Transaction could not be authenticated by either the ACS or Mastercard Mastercard Smart Authentication Stand-In - Attempts	A	kE*	01	211	Merchant gets liability shift
Transaction was not authenticated by either ACS or Mastercard as Acquirer SCA Exemption was applied	I***	kN	06	216	Merchant keeps liability
Recurring transaction successfully authenticated by ACS - Frictionless	Y	kO	07	217	Merchant gets liability shift
Recurring transaction successfully authenticated by ACS - Challenge	Y	kP	07	217	Merchant gets liability shift
Recurring transaction successfully authenticated by Mastercard Smart Authentication Stand-In - Frictionless (low risk)	Y	kC	02	212	Merchant gets liability shift
Recurring transaction successfully authenticated by Mastercard Smart Authentication Stand-In - Frictionless (non-low risk)	A	kE	01	211	Merchant gets liability shift
Recurring transaction could not be authenticated by either the ACS or Mastercard Mastercard Smart Authentication Stand-In - Attempts	A	kE*	01	211	Merchant gets liability shift
Data Only transaction (Message category 80). No Authentication performed by either the ACS or Mastercard Mastercard Smart Authentication	U, RC=80	No AAV	04	214	Merchant keeps liability
AAV Refresh transaction successfully authenticated by ACS	Y	kQ**	02	212	Merchant gets liability shift
Transaction could not be authenticated. Attempts doesn't apply	N	No AAV	00	210	Merchant keeps liability
Transaction rejected by issuer. Authorization should not be attempted	R	No AAV	00	N/A	N/A

* Mastercard DS will support a new Leading Indicators for Attempts starting Q3, 2020 – kF

** Mastercard DS will support this new Leading Indicator starting Q3, 2020

*** Txn Status=I is only supported with version 2.2 of EMV 3DS. For version 2.1 "Txn Status=N" with "Txn Status Reason=81"

Appendix M 3RI Payment Transaction Flow

Below is the 3RI Payment Transaction flow for Version 2.2 (3RI payments are not available for version 2.1) of EMV 3DS for recurring and non-recurring transaction.

3RI Payment Transaction Flow for Version 2.2	182
--	-----

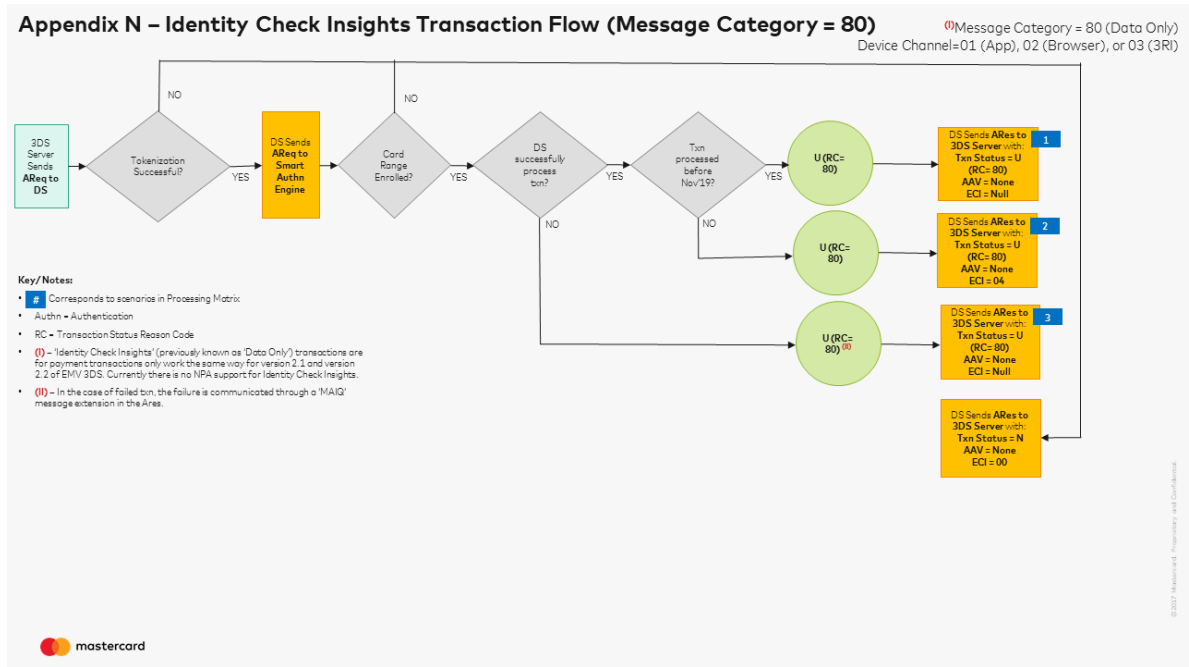
Appendix N Mastercard Identity Check Insights Transaction Flow

The illustration below depicts the positive and negative "Identity Check Insights" payment transaction scenarios in the form of a flow diagram.

Identity Check Insights Transaction Flow.....	184
---	-----

Identity Check Insights Transaction Flow

Below is the Mastercard Identity Check Insights Transaction flow.



Appendix O Security Measures

The Parties will, at a minimum, implement the following types of security measures.

Security Measures Types..... 186

Security Measures Types

This section lists the different types of security measures.

1. Physical Access Control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers, and so forth);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual Access Control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (for example, password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, according to the data processing environment.

3. Data Access Control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;

- Change procedure;
 - Deletion procedure.
4. **Disclosure Control**
Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include
- Tunneling;
 - Logging;
 - Transport security.
5. **Entry Control**
Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include
- Logging and reporting systems;
 - Audit trails and documentation.
6. **Control of Instructions**
Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include
- Unambiguous wording of the contract;
 - Formal commissioning (request form);
 - Criteria for selecting the Processor.
7. **Availability Control**
Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include
- Backup procedures;
 - Mirroring of hard disks (for example, RAID technology);
 - Uninterruptible power supply (UPS);
 - Remote storage;
 - Anti-virus/firewall systems;
 - Disaster recovery plan.
8. **Separation Control**
Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include
- Separation of databases;
 - “Internal client” concept / limitation of use;
 - Segregation of functions (production/testing);
 - Procedures for storage, amendment, deletion, transmission of data for different purposes.

Appendix P Acronyms

Listed in this topic are the acronym terms and descriptions used for the Mastercard Identity Check Program.

3DS.....	190
3RI.....	190
AAV.....	190
ABU.....	190
ACS.....	190
AReq.....	190
ARes.....	190
AuthE.....	190
AuthO.....	190
B2B.....	191
BAU.....	191
BIN.....	191
BPS.....	191
BRN.....	191
CAB.....	191
CAST.....	191
CDCVM.....	191
CIS.....	191
CIT.....	192
CNP.....	192
COF.....	192
CP.....	192
CReq.....	192
CRes.....	192
CVM.....	192
DS.....	192
DTI.....	192
EBA.....	193
ECI.....	193
EEA.....	193
EMV.....	193
GDPR.....	193
GDS.....	193

HTML.....	193
ICA	193
IPM.....	193
KBA	194
KPI.....	194
LVP.....	194
MCC.....	194
MIT.....	194
MLRMP.....	194
MOTO.....	194
MPE.....	194
MRPP	194
MUPP.....	195
OBS.....	195
OOB.....	195
OTP.....	195
PReq.....	195
PRes.....	195
PSD.....	195
PSP.....	195
PwBA.....	195
RBA.....	196
RReq.....	196
RRes.....	196
RTS.....	196
SAFE.....	196
SCA.....	196
SLI.....	196
SPA.....	196
TCC.....	196
TRA.....	197
TXN.....	197
UCAF.....	197
UI.....	197
UX.....	197
VCN.....	197

3DS

Three Domain Secure

3RI

3DS Requestor Initiated (Non-payment and Payment)

AAV

Accountholder Authentication Code

ABU

Automatic Billing Updater

ACS

Access Control Server

AReq

Authentication Request

ARes

Authentication Response

AuthE

Authentication

AuthO

Authorization

B2B

Business-to-Business

BAU

Business as Usual

BIN

Bank Identification Number

BPS

Basis Points

BRN

Banknet Reference Number

CAB

Card Acceptor Business

CAST

Compliance Assessment and Security Testing

CDCVM

Consumer Device Cardholder Verification Method

CIS

Customer Interface Specifications

CIT

Cardholder or Consumer Initiated Transaction

CNP

Card Not Present

COF

Card-On-File

CP

Card Present

CReq

Challenge Request

CRes

Challenge Response

CVM

Cardholder Verification Method

DS

Directory Server

DTI

Digital Transaction Insights

EBA

European Banking Authority

ECI

Electronic Commerce Indicator

EEA

European Economic Area

EMV

Europay Mastercard VISA

GDPR

General Data Protection Regulation

GDS

Global Distribution System

HTML

Hypertext Markup Language

ICA

Interbank Card Association

IPM

Integrated Product Messages

KBA

Knowledge-Based Authentication

KPI

Key Performance Indicator

LVP

Low-Value Payments

MCC

Merchant Category Code

MIT

Merchant-Initiated Transactions

MLRMP

Maestro Low Merchant Risk Program

MOTO

Mail Order Telephone Order

MPE

Member Parameter Extract

MRPP

Maestro Recurring Payment Program

MUPP

Maestro Utility Payment Program

OBS

On-Behalf Service

OOB

Out Of Band

OTP

One Time Password

PReq

Preparation Request

PRes

Preparation Response

PSD

Payment Services Directive

PSP

Payment Service Provider

PwBA

Pay with Bank Account (PwBA) card ranges

RBA

Risk-Based Authentication

RReq

Results Request

RRes

Results Response

RTS

Regulatory Technical Standards

SAFE

System to Avoid Fraud Effectively

SCA

Strong Customer Authentication

SLI

Security Level Indicator

SPA

Secure Payment Application

TCC

Transaction Category Code

TRA

Transaction Risk Analysis

TXN

Transaction

UCAF

Universal Cardholder Authentication Field

UI

User Interface

UX

User Experience

VCN

Virtual Card Number

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively “Mastercard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers “AS IS” and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Information Available Online

Mastercard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on Mastercard Connect™. Go to Publications [Support](#) for centralized information.