Mastercard Click to Pay Program Requirements

10 January 2024

SRCPR

Contents

Summary of Changes, 10 January 2024

This section reflects updates since the previous release.

Description of Change	Where to Look
Updated Card listing requirements	SRCi Requirements
Updated Privacy and Data Protection Requirements	Terms Used in this Guide

Chapter 1 Click to Pay Introduction

This section provides an overview of this document, definitions of key terms used throughout and an overview of the Mastercard Click to Pay Program.

About this Guide

The Mastercard Click to Pay Program identifies the requirements and best practices of Mastercard Click to Pay participants when supporting Mastercard-branded Click to Pay transactions.

The purpose of this guide is to:

- Define the Mastercard Click to Pay Program requirements for supporting Click to Pay transactions with Mastercard-branded products
- Propose recommendations, which constitute best practices for Click to Pay implementations
- Address what is not covered in the EMV[1] Click to Pay Specification, such as explanatory guidance concerning data items to be collected

Audience

This guide is intended for use by participants and their service providers supporting Mastercard Click to Pay.

The target audience includes:

- PSP/Merchant/Acquirer playing the role of SRCi
- Issuer participating in Click to Pay program

Related Publications

The following documents provide information related to the subjects discussed in this document.

EMVCo documents are available online at:

- www.emvco.com/emv-technologies/src/

Mastercard documents are available on Mastercard Connect™ and Brand.Mastercard.com.

- *MDES—Standard Token Implementation Plan for Remote Commerce Programs*
- *Mastercard Rules*
- *MDES—Technical Specifications for Dual and Single Message Systems*
- *Mastercard Brand Mark Guidelines*
- *Digital Secure Remote Payment (DSRP)—Acquirer Implementation Guide*
- *MDES Token Connect - Token Requestor Implementation Guide and Specification*
- *Security Rules and Procedures*

[1] EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.

Requirements and Best Practices

Requirements and best practices are provided throughout this guide, using different conventions, to assist participants when determining if functional elements must be implemented or are Mastercard recommendations.

Requirements are always expressed using the word must. Requirements are contained in tables and are indicated by a capital **R**.

Best practices are Mastercard recommendations for the best ways to implement Click to Pay options. If participants choose not to follow them, their Mastercard Click to Pay implementation will still work but may not be as effective or efficient as it could be. Best practices are written using the word should. Best practices are formatted in the same way as requirements but are preceded by the letters **BP**.

About Click to Pay

Click to Pay is a global specification developed by EMVCo to create an e-commerce experience that aims to deliver the same security, convenience and control currently offered to consumers in the physical world.

As shopping habits shift to digital, consumers expect:

- Security: EMV-like security across all channels and devices
- Convenience: A streamlined, intuitive and consistent payment experience everywhere
- Control: Payment choice and flexibility

Click to Pay[2] enables scale across devices, operating systems, apps and browsers with a standards-based framework.

[2] https://www.emvco.com/wp-content/uploads/2018/10/EMV-SRC-QA_Oct18-FINAL.pdf

Mastercard Click to Pay Role Definitions and Responsibilities

There are defined roles within the Mastercard Click to Pay Program.

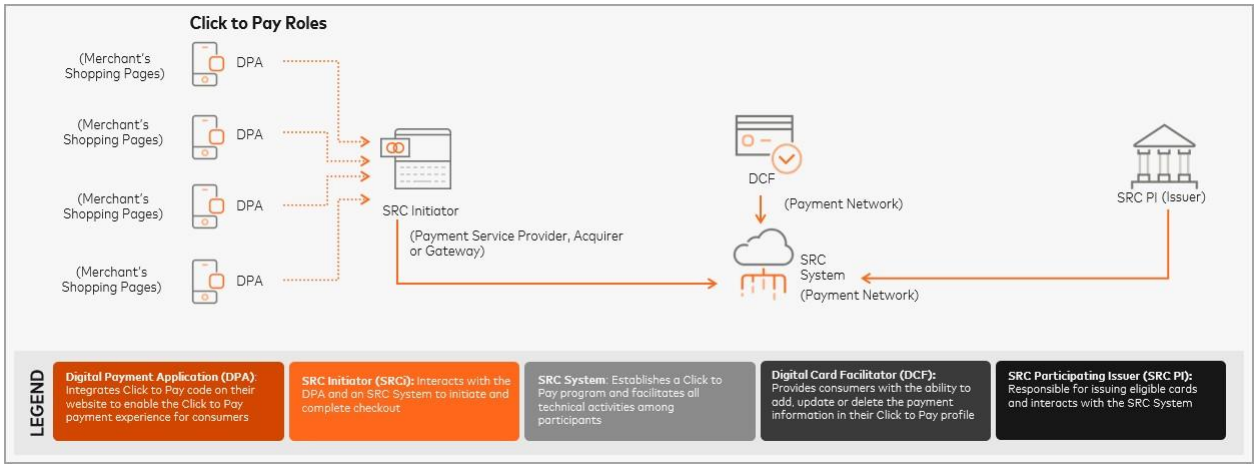
Role	Definition/Responsibilities	Participants
Digital Card Facilitator (DCF)	Provides a consumer with access to a digital card. Provides selected payment card information, collects additional details as required such as consumer ID, address and Cardholder Authentication. • Host UI to display selected card details, capture/display address details, capture/display consumer user ID and contact information • Perform Cardholder Authentication as required • Present relevant Terms and Conditions and collect relevant consumer consent	Types of entities[3] that can play this role include: • Networks
Digital Payment Application (DPA)	A website, web or mobile application operated by the merchant, marketplace, or other service provider where consumer can purchase goods or services. Integrates Click to Pay code on website to enable Click to Pay Payment experience. • Onboard/register and integrate with their preferred SRCi • Display Click to Pay branding Digital Assets • Display appropriate messaging to their consumers	Types of entities[3] that can play this role include: • Merchant • Marketplace

[3] Not an exhaustive list. Representative list of types of entities that are expected to perform these Mastercard Click to Pay roles at the time of initial commercial launch. Additional entities may be included in future versions.

Role	Definition/Responsibilities	Participants
SRC Initiator (SRCi)	Interacts with the DPA and Click to Pay system to initiate and complete checkout. Enables discovery and selection of payment cards. • Onboard with participating Click to Pay Systems • Integrate with Mastercard Click to Pay system/APIs provided by one or more Click to Pay Systems • Register their DPAs with Mastercard Click to Pay system • Build UI/UX to facilitate Click to Pay checkout experience for Mastercards	Types of entities[3] that can play this role include: • Networks • Payment Service Providers/ Gateways • Merchants • eCommerce Service/ Technology Providers • Acquirers
Click to Pay System	Technical platform that facilitates remote card payments.	Types of entities[3] that can play this role include: • Payment Network[4]
Click to Pay Participating Issuer (Click to Pay PI)	Responsible for enrollment of cardholder	Types of entities[3] that can play this role include: • Issuers

How the Roles Work Together

The following is an example of how the different Click to Pay roles work together.



[4] Mastercard is the Click to Pay System for Mastercard-branded products.

Chapter 2 Mastercard Click to Pay Program Requirements

This section contains the requirements that participants must comply with to participate in the Mastercard Click to Pay Program. It also contains best practices to help ensure participants receive the maximum benefit from those implementations. DCF requirements are not included at this time.

Issuer Requirements

This section describes requirements and best practices for issuers that participate in the Mastercard Click to Pay Program.

Authentication Requirements

The following table contains issuer authentication requirements for the Mastercard Click to Pay Program.

Table 1: Legends

Region	Description
Global	Global
EUR	Europe
EEA	European Economic Area
US	United States
Canada	Canada

Requirement or Best Practice?	Functional Element	Description	Region
R	ISS.Authen.R1	Issuers must support cardholder authentication if requested by the Click to Pay system at the time of card enrollment, including card provisioning for Click to Pay Merchant Digital Card-on-File, through Identity Check 3DS NPA (non-payment authentication)	EEA
BP	ISS.Authen.BP1	Issuers should support cardholder authentication if requested by the merchant at the time of transaction through Identity Check (EMVCo 3DS)	Global
BP	ISS.Authen.BP2	Issuers should leverage upon possible SCA exemptions as defined by PSD2 regulation.	EUR
BP	ISS.Authen.BP3	Issuers should consider if there is a need for operational changes related to their fraud systems setup, concerning the introduction of Click to Pay and the monitoring of such transactions.	EUR

Card Art Requirements

The following table contains issuer Card Art requirements for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
R	ISS.CrdArt.R1	Mastercard brand compliant Card Art provided by Issuers participating in MDES must be used for display purposes in all relevant Click to Pay flows. For Issuers not participating in MDES, Mastercard branded generic card art will be used.	Global

Information Requirements

The following table contains issuer information requirements for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
BP	ISS.Info.BP1	Issuers should educate cardholders about the benefits of Click to Pay via all channels available (in-app, email, etc.).	Global

Integration Requirements

The following table contains issuer integration requirements for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
BP	ISS.Integ.BP1	If an Issuer is enrolled with MDES Customer Service APIs, they should update their internal customer servicing portals to reflect Click to Pay.	Global
BP	ISS.Integ.BP2	Issuers are advised to review their current token life cycle management procedures, using MDES CS APIs or their ABU integration, and make additional changes, if needed.	EUR

Onboarding Requirements

The following table contains issuer onboarding requirements for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
BP	ISS.OB.BP1	Issuers should review their pre-digitization rules for Click to Pay. Tokens are provisioned in active state without cardholder authentication when issuer responds APPROVED or REQUIRE_ADDITIONAL_AUTHENTICATION. Click to Pay also supports FPANs provisioning of cards, for Issuers who are not on MDES or BIN ranges that are not enabled for WID 327. **NOTE: Response results in an active token.**	Global
BP	ISS.OB.BP2	Issuers are advised to review their current token life cycle management procedures, using MDES CS APIs or their ABU integration, and make additional changes, if needed.	Global

Consumer Enrollment with Push Provisioning Requirements

The following table contains issuer requirements for consumer enrollment with Push Provisioning in the Mastercard Click to Pay Program.

NOTE: Additional data sharing agreements may need to be executed between Mastercard and Issuers for other regions.

Requirement or Best Practice?	Functional Element	Description	Region
R	ISS.Push.R1	If issuers leverage Token Connect API, issuers must perform strong cardholder authentication prior to initiating Click to Pay push provisioning and not send Yellow Path/Require Additional Authentication during Click to Pay push provisioning.	Global
R	ISS.Push.R2	Issuers SCA must be PSD2-compliant.	EEA, United Kingdom

Requirement or Best Practice?	Functional Element	Description	Region
R	ISS.Push.R3	Issuers allowing consumers to add cards to Mastercard Click to Pay must agree to send relevant Personally Identifiable Information (full name, billing address, email address and mobile number) that is required to create a Click to Pay profile. Additionally, issuers must pass the consumer locale information in the URI so Click to Pay can drive the correct experience for the consumer.	Global
R	ISS.Push.R4	If the issuer implements Token Connect, they must supply PII data along with card data. This data includes full name, billing address, email address and mobile number.	EUR
BP	ISS.Push.BP1	Issuers should offer their cardholders the capability to add cards to Click to Pay ahead of checkout by leveraging the Token Connect API.	Global
R	ISS.Push.R5	Issuers deploying the Mastercard Token Connect service for their customers to push provision tokens into Click to Pay shall adopt and comply with the data privacy provisions in Data Processing Matters.	Global

SRCi Requirements

This section describes requirements and best practices for the SRCi role in the Mastercard Click to Pay Program.

Digital Payment Application

The SRCi is responsible for ensuring the Digital Payment Application (DPA) complies with the following table containing requirements for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.DPA.R1	DPA must ensure that it complies with applicable DPA and merchant requirements which are part of this program rules. DPA must ensure it complies with applicable DPA and merchant requirements which are part of these program rules. DPA is liable to Mastercard for any noncompliance by their DPA's or the merchant.	Global
R	SRCI.DPA.R2	A DPA must adhere to Click to Pay Icon and Assets requirements (refer to Click to Pay Icon and Assets section in this document).	Global
R	SRCI.DPA.R3	A DPA must ensure that it has, at a minimum, provided a privacy notice and all other appropriate disclosures and terms to, as well as have obtained any necessary consents from, a cardholder in order to have a valid legal basis to collect and share any personal information with the Mastercard Click to Pay System, Mastercard SRCi, Mastercard DCF or other related Mastercard system or other third-party Click to Pay participant or role within the Click to Pay ecosystem as provided in this document.	Global
R	SRCI.DPA.R4	DPAs may route debit transactions to any network enabled on the card.	US
R	SRCI.DPA.R5	On transactions routed to Mastercard, the DPA must elect one of the following Mastercard-enabled Tokenization models: • Digital Secure Remote Payment (DSRP) • Dynamic Token Verification Code (DTVC)	Global

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.DPA.R6	A participating DPA must only collect, use and share such personal information in support of • a Click to Pay role, held by Mastercard (i.e. Click to Pay system, SRCi or DCF), or any Mastercard related system • other third-party Click to Pay participant/role, as provided in this document or the EMVco Click to Pay Standard and for the facilitation of a payment at the direction of a cardholder. Participating DPA must not retain any personal information for longer than is required to accomplish the aforementioned purpose(s) and must not use any personal information other than to accomplish such purpose(s) without first having obtained express consent from the cardholder.	Global
R	SRCI.DPA.R7	For Merchant Digital Card on File, the DPA must ensure the merchant: • Requires cardholder to create an account with the merchant. • Is solely responsible for and has appropriate MDC Terms and Conditions in place with cardholder. • Has obtained and maintains appropriate records of MDC Consents. • Limits use of Merchant Digital Card on File solely for use with merchant. • Be solely responsible for the payment credential received through Merchant Digital Card-on-file. • Be responsible for addressing and resolving cardholder inquiries relating to Merchant Digital Card on File.	

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.DPA.R8	For utilization of an MDC Identifier received through Merchant Digital Card-on-file for purposes of furnishing such credentials to alternative card-on-file solutions, must ensure merchant: • Be solely responsible for entering into and complying with all terms and conditions required for the utilization of an alternative card-on-file solution with the applicable provider. • Be solely responsible for merchant's use such alternative card-on-file solution	

User Interface

The following table contains the SRCi user interface requirements and best practices for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.UI.R1	The SRCi/DPA must adhere to Click to Pay icon and asset requirements (refer to the Click to Pay Icons and Assets section in this document)	Global
R	SRCI.UI.R2	The SRCi must provide user the ability to access Click to Pay profile using email ID and new user checkout with Click to Pay.	Global
R	SRCI.UI.R3	The SRCi must provide user the ability to add card through new user checkout or existing user profile.	Global
R	SRCI.UI.R4	The SRCi must collect card information as part of card enrolment. Card information includes collection of FPAN, expiration date and security code.	Global
R	SRCI.UI.R5	The SRCi must display all cards returned by Mastercard Click to Pay system.	Global
R	SRCI.UI.R6	The SRCi must display the card list if there is more than one card returned.	Global

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.UI.R7	The SRCi must display card details in the way that is returned by the Click to Pay system. Card details includes the following elements: • Card art • Card program name • Last 4-digits of card number • Card benefit message as part of Digital Card Feature	Global
R	SRCI.UI.R8	The SRCi must adhere to the following requirements for display of card benefit message • Card benefit message must be displayed as text-only • Should not include interactive features or visuals (for example, iconography, logo and imagery) • Text must be limited to two lines or maximum 74 characters in the most common viewport width (480px)	Global
R	SRCI.UI.R9	If the SRCi retrieves multiple cards, including cards from multiple Click to Pay systems, it must display them according to the hierarchy: • The first set of card(s) at the top of the list must be in descending order of last used time stamp sent across all Click to Pay system. For example, the most recent used card must be displayed first, followed by the card used prior to that, and so forth • The next set of card(s)must be in order of first added time stamp sent across by all Click to Pay systems. For example, the card enrolled first in the user profile will be displayed first, followed by the card added next based on date and time**.** These are cards that are available in the user's profile but have not been used for a transaction An exception may be made in the case of the display of a merchant co-brand card when the consumer is shopping at that particular merchant. In this instance SRCi may display the merchant co-brand card at the top of the list.	Global
R	SRCI.UI.R10	The SRCi must redirect user automatically to DCF if there is only one card returned by Click to Pay system(s).	Global

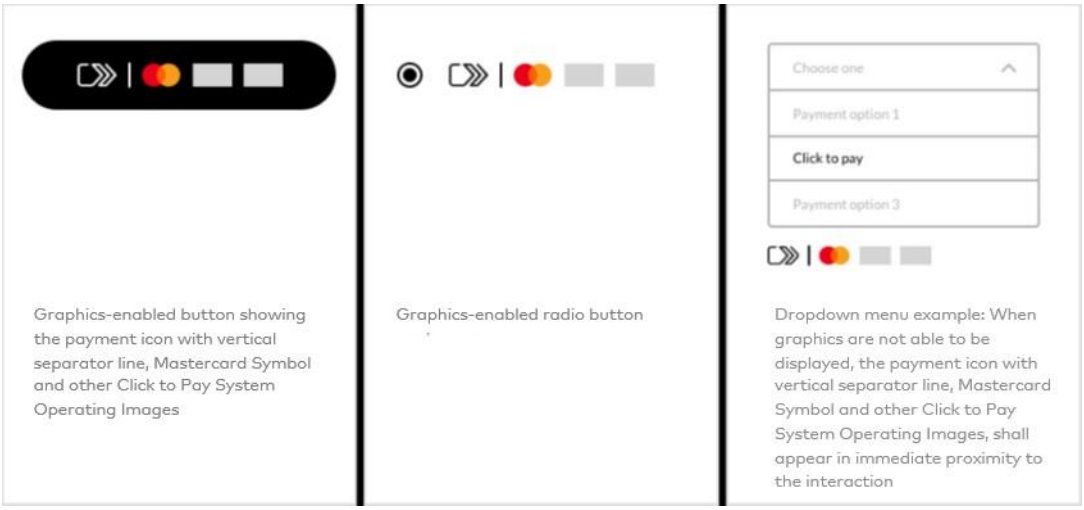
Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.UI.R11	If Click to Pay trusted device cookie is present and validated by Click to Pay systems(s), SRCi must proceed with the recognized user checkout flow (Refer to Mastercard Developers for more details).	Global
R	SRCI.UI.R12	Upon email ID entry by user and recognition by Click to Pay system(s), SRCi must be able to facilitate One Time Password (OTP) entry to validate the user.	Global
R	SRCI.UI.R13	During user validation through One Time Password (OTP), SRCi must be able to communicate failed OTP submission to the user.	Global
R	SRCI.UI.R14	During user validation through One Time Password (OTP), SRCi must be able to provide fallback checkout option to user if user has failed maximum number of attempts determined by Click to Pay system.	Global
R	SRCI.UI.R15	During user validation through One Time Password (OTP), SRCi must provide ability to resend OTP code via email and/or phone in case user is experiencing an issue completing OTP.	Global
R	SRCI.UI.R16	The SRCi must support Click to Pay experience within the current and last 2 versions of the following browsers and device channel: **Web** • Safari • Chrome • Microsoft Edge • Firefox • Android Browser **Mobile** • Android KitKat • iOS • Chrome • Firefox • Safari	Global
R	SRCI.UI.R17	The SRCi must display Legal and Privacy disclaimer if not included in DPA's terms and privacy notice.	Global

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.UI.R18	The SRCi must provide user the ability to navigate from Click to Pay experience and return to the DPA experience.	Global
BP	SRCI.UI.BP1	If billing address is required by DPA and/or local market, the SRCi should collect billing address information in addition to other card information.	Global
BP	SRCI.UI.BP2	When describing 'Click to Pay', the SRCi should be concise and human. (for example, "Check out faster with Click to Pay".) The SRCi should limit the value proposition to no more than two lines.	Global
BP	SRCI.UI.BP3	Instructional text and error messaging associated with data collection should provide clear action and resolutions.	Global
BP	SRCI.UI.BP4	The next step of enrolment needs to be accessible after card information has been collected.	Global
BP	SRCI.UI.BP5	In the event more than 10 cards are returned by Click to Pay system(s), the SRCi should introduce asynchronous loading to ensure user has access to all cards returned.	Global
BP	SRCI.UI.BP6	The SRCi should indicate actions to progress forward in the experience (for example, call-to-action buttons indicating 'Continue', 'Sign In' etc.)	Global

Click to Pay Icon and Assets

This section includes requirements for representation of EMV® Click to Pay payment mark otherwise known as the 'Click to Pay assets'. The presence of the Click to Pay icon in a trigger or

non-trigger format provides the starting point for a Click to Pay enabled experience and is placed on the Digital Payment Application.



Requirement or Best Practice?	Functional Element	Description	Region
R	SRCi.IA.R1	At least one brand element of Click to Pay must be positioned prominently on SRCi UI to drive brand awareness and understanding that Click to Pay is a payment option. Any combination of brand elements below is acceptable: • Horizontal mark • "Click to Pay" written as text • Click to Pay icon (Vertical mark)	Global
R	SRCi.IA.R2	Click to Pay icon and asset display in either trigger or non-trigger format must be as per Mastercard's internal program brand requirements, refer to *Signaling Mastercard Click to Pay enablement* on Brand Center.	Global
R	SRCi.IA.R3	Click to Pay asset must be displayed in equal size and parity with other payment logo in DPA checkout UI.	Global
R	SRCi.IA.R4	Click to Pay icon and asset display must follow web color contrast and accessibility standards as per their market compliance.	Global

Security and Privacy Requirements

The following table contains SRCi security and privacy requirements and best practices for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.SP.R1	A participating SRCi must ensure that they have, at a minimum, provided a privacy notice and all required and appropriate disclosures in accordance with Privacy and Data Protection Requirements. A participating SRCi must ensure they have obtained all necessary authorizations and consents from cardholders or otherwise ensure they have a valid legal basis under Privacy and Data Protection Requirements, to share any Personal Data with the Mastercard Click to Pay System, Mastercard SRCi, Mastercard DCF or other related Mastercard system or other third-party Click to Pay participant or role within the Click to Pay ecosystem as provided in this document.	Global
R	SRCI.SP.R2	A participating SRCi must only collect, use and share Personal Data in support of: • a Click to Pay role, held by Mastercard (i.e. Click to Pay system, SRCi or DCF), or any Mastercard related system • other third-party Click to Pay participant/role, as provided in this document or the EMVco Click to Pay Standard • for the facilitation of a payment at the direction of a cardholder. A participating SRCi must not retain any Personal Data for longer that is required to accomplish the aforementioned purpose(s) and must not use Personal Data other than to accomplish such purpose(s).	Global
R	SRCI.SP.R3	The SRCi must not store any data returned as part of the Click to Pay checkout payload from Mastercard without explicit consumer consent.	Global
R	SRCI.SP.R4	The SRCi must be compliant with the PCI Data Security Standard (PCI DSS).	Global

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.SP.R5	(a) Each SRCi must inform Mastercard in writing of any Account Data Compromise Event, or a potential Account Data Compromise Event (each defined in *Mastercard Security Rules and Procedures*), in accordance with the account data compromise event procedures set forth in Chapter 10 of *Mastercard Security Rules and Procedures* and any other applicable Standards, within the timeframes set forth therein. (b) Each SRCi shall be solely responsible for any notices to Data Subjects as a result of any Account Data Compromise Event, as and to the extent required by applicable Privacy and Data Protection Requirements.	Global
R	SRCI.SP.R6	Each SRCi must align to industry best practices to ensure that malware is not coded or introduced into their respective systems interacting with Mastercard's Click to Pay.	Global
R	SRCI.SP.R7	Each SRCi must continue to review, analyze and implement improvements to and upgrades of its malware prevention and correction programs and processes that are consistent with all PCI DSS requirements as a Level 1 Service Provider. If malware is found to have been introduced into the program or Mastercard's or Customer's systems interacting therewith, Mastercard and the affected Customer(s) will cooperate and use efforts to promptly communicate, and diligently work to remedy the effects of the malware, in each case, in accordance with the account data compromise event procedures set forth in Chapter 10 of *Mastercard Security Rules and Procedures* and any other applicable Standards	Global
BP	SRCI.SP.BP1	The SRCi should support capabilities to regulate untrusted user log in requests.	Global

Requirement or Best Practice?	Functional Element	Description	Region
BP	SRCI.SP.BP2	It is Mastercard's expectation that SRCi programs will follow industry best practices with regards to their software development lifecycle and the security of their applications and platform. This includes but is not limited to the areas of: authentication and authorization (authN/Z), protection of data 'AT REST' and 'IN TRANSIT', security event auditing and logging, data validation, web client and server configurations. **NOTE: Additional security requirements and best practices may be added in upcoming revisions.**	Global

Onboarding and Integration Requirements

The following table contains the SRCi onboarding and integration requirements for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.OI.R1	The SRCi must register all the DPAs/ merchants under it via the Mastercard Click to Pay DPA Registration API.	Global
R	SRCI.OI.R2	The SRCi must update the Mastercard Click to Pay with all changes that have been made to DPA records (this includes, but is not limited to: merchant name, merchant category code, acquirer ID, merchant ID).	Global
R	SRCI.OI.R3	An SRCi that registers merchants with Mastercard Click to Pay must have implemented a sanctions compliance program.	Global
R	SRCI.OI.R4	The SRCi must integrate with the latest and approved version of Mastercard Click to Pay SDK and the required APIs, including Confirmation API. Refer to Mastercard Developers for technical details.	Global

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.OI.R5	The SRCI must integrate with the approved Mastercard Click to Pay SDK and the required APIs (Payload API and Confirmation API.) Refer to *SRCi Technical Implementation and Integration Guide*.	Global
R	SRCI.OI.R6	An SRCi must comply with all required elements of the current version of Mastercard Click to Pay (including the API specifications) and satisfy any testing and certification or re-certification requirements that may be imposed by Mastercard from time to time. Mastercard will provide a SRCi participating in the program with notice of any new features or functionality or modification to the API specifications prior to the release of those features in the live production environment.	Global
R	SRCI.OI.R7	An SRCi will have six months from the time the new functionality is released in production to implement any necessary system changes required by the new version of the specification which is available on Mastercard Developers. Re-certification will be required at Mastercard's discretion, not more frequently than once every 12 months. Mastercard reserves the right to shorten compatibility support period to correct a specific security issue or for emergency update.	Global
R	SRCI.OI.R8	SRCi must support DSRP or DTVC for all use cases included Merchant Initiated, split shipment, credential on file, etc. For DSRP refer to *Digital Secure Remote Payment Acquirer Implementation Guide*.	Global
R	SRCI.OI.R9	If SRCi/DPA should consider leveraging any possible acquirer SCA exemptions as defined by PSD2 regulation using the Payload returned by Mastercard Click to Pay system.	EEA, United Kingdom
R	SRCI.OI.R10	When SRCi received DSRP payloads, the downstream acquirer must populate the DSRP cryptogram within DE104, during authorization.	EUR
R	SRCI.OI.R11	For each transaction, after receiving payload from the Click to Pay system, SRCi must initiate EMV 3DS Transaction Authentication, in order to comply with PSD2 regulation.	EEA, United Kingdom

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.OI.R12	SRCi must comply with all applicable laws and regulations, including the Code of Conduct for the Credit and Debit Card Industry in Canada.	Canada
R	SRCI.OI.R13	Merchants/PSPs/Acquirers must validate card authentication status flag retrieved in Payload. In case SCA was not performed during card add to Click to Pay, Payment Authentication must be triggered during checkout always, regardless of available exemptions.	EEA, United Kingdom
R	SRCI.OI.R14	SRCi's must be enrolled in and approved to participate in Mastercard's Click to Pay Program in order to perform SRCi activities.	EUR
BP	SRCI.OI.BP1	When SRCi received DSRP payloads, the downstream acquirer must populate the DSRP cryptogram within DE104, during authorization.	Global

Examination and Audit

The following table contains the SRCi examination and audit requirements for the Mastercard Click to Pay Program.

NOTE: For third-party SRCis in EUR, there may be a potential need for additional regulatory terms and oversight processes to comply with local laws.

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.EA.R1	Mastercard reserves the right to conduct an audit or examination of any SRCi or SRCi provider to ensure full compliance with the Program requirements mentioned in this document and the technical requirements referred on Mastercard Developers. Any such audit or examination is at the expense of the SRCi, and a copy of the audit or examination results must be provided promptly to Mastercard upon request. For the avoidance of doubt, should a SRCi provider be unable or unwilling to cover the cost of such audit or examination, the audit or examination shall be at the responsible SRCi's expense. Mastercard shall not exercise this right more than once a year unless Mastercard has reason to believe that the SRCi does not materially comply with the Program requirements mentioned in this document and the technical requirements referred on Mastercard Developers.	Global

Performance Requirements

The following table contains the SRCi performance requirements for the Mastercard Click to Pay Program.

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.PF.R1	There must be error handling at the system level in the event that a call has failed in a critical/fatal manner to make the consumer aware.	Global
BP	SRCI.PF.BP1	The SRCi should enable best-in-class experience (UI availability and performance) for end users interacting with the application. **NOTE: Additional performance requirements may be added in upcoming revisions.**	Global

Reporting Requirements

The following table contains the SRCi reporting requirements for the Mastercard Click to Pay Program.

NOTE: All metrics should be at a DPA level, on a monthly basis.

Requirement or Best Practice?	Functional Element	Description	Region
R	SRCI.RPT.R1	Number of Mastercard transactions completed (postbacks)	Global

NOTE: Additionally, SRCi should capture any error states received from Mastercard Click to Pay and report those on an as-needed basis for troubleshooting purposes.

Data Processing Matters

This section applies to the Processing of Personal Data by any Click to Pay Participating Issuer and Mastercard (collectively referred to as "the Parties") to provide the Click to Pay Push Provisioning Service ("Service") and supplements any existing privacy and data protection terms contained in the Mastercard Click to Pay Program Requirements pertaining to the Processing of Personal Data.

In case of conflict, the privacy and data protection terms of this Chapter shall prevail. Capitalized terms not otherwise defined herein have the meaning given to them in the Mastercard Click to Pay Program Requirements. In the event of a conflict, the definitions provided in this Chapter shall prevail.

Roles of the Parties

With regard to the Processing of Personal Data in the context of the Service, the Parties acknowledge and confirm that neither Party acts as a Processor on behalf of the other Party; and that each Party is an independent Controller; and that the Mastercard Click to Pay Program Requirements does not create a joint-Controllership or a Controller-Processor relationship between the Parties. The Parties acknowledge and agree that the scope of each Party's role as independent Controller is as follows:

- Click to Pay Participating Issuer is a Controller for any Processing for the purpose of displaying the Service to Data Subjects in Click to Pay Participating Issuer banking applications and transmitting Personal Data to Mastercard for the Service via MDES Token Connect API.
- Mastercard is a Controller for any Processing for the purpose of operating, developing, improving, maintaining, marketing and providing the Click to Pay Service to Data Subjects, and for internal research, fraud, security and risk management.

Compliance with Privacy, Data Protection and Information Security Requirements

Each Party shall comply and shall have any subcontractor comply with applicable Privacy, Data Protection and Information Security Requirements and shall perform its obligations under this Mastercard Click to Pay Program Requirements in compliance with all Privacy, Data Protection and Information Security Requirements.

As used herein, "Privacy, Data Protection and Information Security Requirements" means all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements relating in any way to the privacy, data protection, confidentiality, or security of Personal Data, including, without limitation, the Europe General Data Protection Regulation 2016/679 ("GDPR"); 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 California Consumer Privacy Act (CCPA); the Gramm-Leach-Bliley Act; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws regulating banking secrecy and outsourcing requirements; laws regulating international data transfers and/or on-soil requirements; laws regulating incident reporting and data breach notification requirements, including guidelines and recommendations from the competent regulators; all other similar international, federal, state, provincial, and local requirements; the Payment Card Industry ("PCI") Data Security Standards; and all applicable provisions of the parties' written information security policies, procedures and guidelines.

Legal Ground and Notice

Click to Pay Participating Issuer must rely on a valid legal ground for, 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 in the context of the Service.

In particular, Click to Pay Participating Issuer represents and warrants that it shall obtain any necessary consents, authorizations and permissions for the collection, use, disclosure, transfers and any other Processing of Personal Data by Click to Pay Participating Issuer and Mastercard in the context of the Service, to the extent and in the manner required by applicable Privacy, Data Protection and Information Security Requirements. Upon request from Mastercard, Click to Pay Participating Issuer must demonstrate that it relies on a valid legal ground for the Processing, including consent, where applicable. Click to Pay Participating Issuer also confirms and warrants that it will inform Data Subjects in particular of the transfer and storage by Mastercard of their Personal Data outside the country in which it was collected (e.g. transfer to and storage in the United States), the ways in which their Personal Data will be Processed by Click to Pay Participating Issuer and Mastercard and any other information required by applicable Privacy, Data Protection and Information Security Requirements.

Data Subject Requests

The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Personal

Data under Privacy, Data Protection and Information Security Requirements with regard to Personal Data Processed by Click to Pay Participating Issuer or Mastercard for the Service.

Data Integrity

Click to Pay Participating Issuer is exclusively responsible for the accuracy, completeness, relevance and integrity of all Personal Data provided to Mastercard.

Assessments

Click to Pay Participating Issuer represents and warrants that it shall conduct and review any relevant assessments (including security or privacy impact assessments) as may be required by applicable Privacy, Data Protection and Information Security Requirements for purposes of implementing the Service, including in respect of any cross-border transfers of Personal Data.

Governmental Requests for Personal Data

Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Click to Pay Participating Issuer shall promptly inform Mastercard in writing if any competent authority, regulator or public authority of any jurisdiction requests disclosure of, or information about, Personal Data that has been Processed solely in connection with the Service.

Click to Pay Participating Issuer shall, without limiting its rights under applicable law, cooperate with Mastercard as reasonably necessary to comply with any direction or ruling made by such authorities.

Information Security

The Parties shall develop, implement, maintain and adhere to a comprehensive written information security program designed to ensure compliance with all applicable Privacy, Data Protection and Information Security Requirements.

Without limitation, each Party's 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 or suspected unauthorized Processing, loss, use, disclosure or acquisition of or access to any Personal Data Processed in connection with the Service ("Information Security Incident")

Each Party's information security program shall, among other things, include regular testing or otherwise monitoring of the effectiveness of its information safeguards. In addition, each Party shall comply with all provisions of its written information security policies, procedures and guidelines which the Parties have mutually agreed are applicable to the Service under the Mastercard Click to Pay Program Requirements.

Information Security Incident

To the extent required by Privacy, Data Protection and Information Security Requirements, each Party shall inform the other Party in writing in a commercially reasonable timeframe, and in any event, no later than the time period required under applicable Privacy, Data Protection, and Information Security Requirements, of any known Information Security Incident involving Personal Data Processed in connection with the Service.

Such notice shall describe, in reasonable detail, the nature and the effect on the other Party, if known, 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. The Party experiencing the Information Security Incident shall promptly take all necessary corrective actions, and shall cooperate with the other Party in all reasonable and lawful efforts to mitigate the effects of such Information Security Incident. Click to Pay Participating Issuer shall obtain Mastercard's approval prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Information Security Incident that expressly mentions Mastercard or its affiliates.

Data Transfer and Storage

Click to Pay Participating Issuer acknowledges and agrees that all data including Personal Data Processed in connection with the Mastercard Click to Pay Program Requirements shall be transferred and stored outside the country in which such Personal Data was collected (e.g. transfer to and storage in the United States), and Click to Pay Participating Issuer represents and warrants that it shall have all necessary consents, authorizations, permissions and/or approvals for such transfer, storage and Processing of all data including Personal Data outside the country in which such Personal Data was collected (e.g. transfer to and storage in the United States), in accordance with applicable Privacy, Data Protection and Information Security Requirements.

EUR Data Protection Law

EUR Data Protection Law regulates the Processing of Personal Data of Data Subjects subject to EUR Data Protection Law by the Parties in the context of the Service provided under the Mastercard Click to Pay Program Requirements.

EUR Data Protection Law supplements the privacy and data protection terms contained in these Mastercard Click to Pay Program Requirements to the extent they pertain to the Processing of Personal Data subject to EUR Data Protection Law. In case of a conflict, the provisions of EUR Data Protection Law shall prevail to the extent of the conflict.

1. Roles of the Parties With regard to the Processing of Personal Data in the context of the Service, the Parties acknowledge and confirm that neither Party acts as a Processor on behalf of the other Party; and that each Party is an independent Controller; and that the Mastercard Click to Pay Program Requirements does not create a joint-Controllership or a Controller-Processor relationship between the Parties. The Parties acknowledge and agree that the scope of each Party's role as independent Controller is as follows:

1.1 Click to Pay Participating Issuer is a Controller for any Processing for the purpose of displaying the Service to Data Subjects in Click to Pay Participating Issuer banking applications and transmitting Personal Data to Mastercard for the Service via MDES Token Connect API.

1.2 Mastercard is a Controller for any Processing for the purpose of operating, developing, improving, maintaining, marketing and providing the Click to Pay Service to Data Subjects, and for internal research, fraud, security and risk management.

2. Obligations of the Parties

Each party is responsible for compliance with EUR Data Protection Law in relation to the Processing of Personal Data for which it is a Controller. Notwithstanding the above, Click to Pay Participating Issuer represents and warrants that, with regard to any Processing of Personal Data of its end users under these Mastercard Click to Pay Program Requirements, including the Processing for which Mastercard is the Controller, it:

2.1 Relies on a valid legal ground under EUR Data Protection Law for each of its Processing purposes, including obtaining Data Subjects' appropriate consent if required or appropriate under EUR Data Protection Law.

2.2 Provides appropriate notice to the Data Subjects regarding

- the Processing of Personal Data, in a timely manner and at the minimum with the elements required under EUR Data Protection Law, and
- as appropriate, data transfers outside of Europe and the existence of the Mastercard BCRs, including the Data Subjects' right to enforce Mastercard BCRs as third-party beneficiaries.

2.3 Takes reasonable steps to ensure that Personal Data is accurate, complete and current; adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;

2.4 Responds to Data Subjects' requests to exercise their rights to

- access
- rectification
- erasure
- data portability
- restriction of Processing
- objection to the Processing, and
- the rights related to automated decision-making and profiling if and as required under EUR Data Protection Law. Click to Pay Participating Issuer agrees and warrants that it will respond to such requests only in consultation with Mastercard. Mastercard agrees to cooperate with Click to Pay Participating Issuer in responding to such requests.

2.5 Limit its Processing of Personal Data to the Processing that is necessary for the purpose of Click to Pay Participating Issuer's fraud countermeasures

that rely on information the Click to Pay Participating Issuer receives via the Service.

3. Data Transfers

Each Party represents and warrants that, in relation to its Processing of Personal Data in the context of the Services:

3.1 Click to Pay Participating Issuer may transfer the Personal Data Processed in connection with the Services outside of Europe in accordance with EUR Data Protection Law.

3.2 Mastercard may transfer the Personal Data Processed in connection with the Services 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 EUR Data Protection Law. Mastercard represents and warrants that it will abide by the Mastercard BCRs when Processing Personal Data in the context of the Services.

4. Data Disclosures

The Parties represent and warrant that they will only disclose Personal Data Processed in the context of the Service in accordance with EUR 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 Mastercard Click to Pay Program Requirements. Mastercard represents and warrants that it will only disclose Personal Data in accordance with the Mastercard BCRs.

5. Security of the Processing; Confidentiality; and Personal Data Breach

5.1 The Parties must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures in accordance with *Description of the Processing Activities Appendix* to ensure a level of security appropriate to the risk, and as appropriate:

- the pseudonymization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In assessing the appropriate level of security, the Parties must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful

destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

5.2 The Parties must 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, and if applicable Process Personal Data in accordance with the Controller's instructions.

5.3 Each Party must notify the other party a Personal Data Breach that relates to Personal Data Processed in the context of the Service and for which the other Party is a Controller, without undue delay, and no later than forty-eight (48) hours after having become aware of a Personal Data Breach. The Parties will assist each other in complying with their obligations to notify a Personal Data Breach. The Party which became aware of a Personal Data Breach will notify, without undue delay and, where feasible, not later than 72 hours after having become aware of it, the competent supervisory authority, where required by EUR Data Protection Law. When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects or upon the competent supervisory authority's request to do so, such Party must communicate the Personal Data Breach to the Data Subject without undue delay, where required by EUR Data Protection Law.

5.4 The Parties will use their best efforts to reach an agreement on whether and how to notify persons or entities of a Personal Data Breach, and must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial action taken.

6. Data Protection and Security Audit

Each Party commits to conduct audits on a regular basis to control compliance with EUR Data Protection Law, including the security measures provided under *5.1 Security of the Processing; Confidentiality; and Personal Data Breach* of EUR Data Protection Law, 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 summary of the audit reports demonstrating its compliance with EUR Data Protection Law obligations and these Mastercard Click to Pay Program Requirements, and as applicable Mastercard BCRs, after redacting any confidential and commercially sensitive information; and
- 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.

7. Liability

Subject to the liability clauses in the Mastercard Click to Pay Program Requirements, each Party agrees that it will be liable towards Data Subjects for the entire damage resulting from a violation of EUR Data Protection Law with regard

to Processing of Personal Data for which it is a Controller. Where the Parties are involved in the same Processing and where they are responsible for any damage caused by the Processing of Personal Data, both Click to Pay Participating Issuer and Mastercard may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Mastercard paid full compensation for the damage suffered, it is entitled to claim back from Click to Pay Participating Issuer that part of the compensation corresponding to Click to Pay Participating Issuer 's part of responsibility for the damage.

8. Applicable Law and Jurisdiction

The Parties agree that EUR Data Protection Law and the Processing of Personal Data under EUR Data Protection Law will be governed by the laws of Belgium and that any dispute will be submitted to the Courts of Brussels.

Appendix A Terms and Processing Activities

The appendix outlines the terms are used and provides a description of the processing activities.

Terms Used in this Guide

The following terms are used in this manual.

Term	Definition
EMVCo 3DS	A fraud prevention system designed for e-commerce sites to facilitate secure online transactions by authenticating a cardholder's identity at the time of purchase.
API	An Application Programming Interface (API) is a software intermediary that allows two applications to send and receive information.
Best Practice (BP)	A recommended act that will improve the Click to Pay experience, but not one that is required.
Card Add	The process where the Consumer adds a card for the purpose of payment.
Card Art	The digital image of the card used to represent the cardholder's card in digital interfaces. When a Mastercard account is represented in any digital payment application, refer to brand.mastercard.com **> Mastercard Brand Mark Guidelines** > **Use in Digital Payments**.
Cardholder Authentication	This is the process that confirms that the individual making a purchase is entitled to use the Payment Card selected. Cardholder Authentication can be performed by the Card Issuer or their agent via technologies such as 3-D Secure.
Click to Pay	Click to Pay is a method of performing a secure purchase for goods or services during a digital or remote shopping experience that involves a merchant checkout, and a consumer device. Unless otherwise clearly indicated, Click to Pay means a Click to Pay participant in the Mastercard Click to Pay Program.
Click to Pay Payment Icon	The EMV® Click to Pay payment icon that is a trademark of EMVCo, LLC that is used to signal that a remote-commerce channel offers payments enabled by the EMV® Secure Remote Commerce specification.

Term	Definition
Click To Pay Program Requirements	The list of requirements and best practices for the Click to Pay Program. This list applies to the Program's: Issuers, SRCIs and DPAs.
Click to Pay Icon & Assets	Click to Pay Icon & Assets means a button, radio button, or drop-down payment selection that triggers a Click to Pay enabled transaction.
Controller	The entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.
Cookie Consent	Consenting to the usage of cookies, which are small data files used to store consumer's information in their web browsers.
Data Subjects	A Cardholder or other natural person whose Personal Data are processed in the context of the Mastercard Click to Pay Program Requirements.
Digital Card Facilitator (DCF)	The Digital Card Facilitator (DCF) provides selected payment card information and collects additional details as required such as: consumer ID, address and Cardholder Authentication.
Digital Card Feature	Digital Card Feature is defined as a card benefit (not as a one-time promotion or offer) that is displayed to the user at the time of checkout within Click to Pay.
Digital Secure Remote Payment (DSRP)	Mastercard generates a unique cryptogram associated with the token for each DSRP transaction
Digital Shopping Application (DPA) / Digital Payment Application (DPA)	The Digital Payment Application or Digital Shopping Application is a website or mobile application operated by the merchant, marketplace, or other service provider where consumer can purchase goods or services.
Dynamic Token Verification Code (DTVC)	Mastercard generates a unique CVC2 value and expiration date for each DTVC tokenized transaction
Email ID	A user's Click to Pay Program account. Unless otherwise clearly indicated, means an Email ID participating in the Mastercard Click to Pay Program.

Term	Definition
EUR Data Protection Law	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).
Europe	The EEA, Switzerland, Monaco and the United Kingdom.
Mastercard Binding Corporate Rules (BCR)	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
Mastercard Digital Enablement Service (MDES)	Mastercard Digital Enablement Service (MDES) allows issuers and merchants to manage Tokenization and digitization to create EMV-like security for every transaction.
MDES Token Connect	MDES Token Connect is the framework allowing the connection of MDES Issuers with open-loop MDES Token Requestors (such as wallets storing tokens on the mobile device or an IoT device, or commerce platforms) in support of Push Provisioning.
Mastercard Click to Pay Cookie	Small data files used to store consumer's Click to Pay identifier in their trusted web browsers in order to facilitate a quick and easy Click to Pay payment experience.
Merchant Digital Card-on-File Consents	Cardholder consents for Merchant Digital Card-on-File which include, but are not limited to, cardholder consents to (i) the MDC Terms and Conditions, (ii) designate a payment credential as a merchant digital card-on-file, and (iii) allow recurring payments to be made using the merchant digital card-on-file.

Term	Definition
Merchant Digital Card-on-File Identifier	With regard to Mastercard branded cards (i) payment Card Data returned by the SRCi, and with regard to non-Mastercard branded cards, (i) a unique identifier that is not Card Data or a token but is a static identifier regardless of whether or not the payment card is tokenized, provided such unique identifier will not be updated in the event the original associated payment card is updated resulting in the need for the cardholder to potentially readd such payment credential as a merchant card-on-file.
Merchant Digital Card-on-File Terms and Conditions	The terms and conditions between a merchant and cardholder for Merchant Digital Card-on-File which include MDC Consents and other requirements set forth in these Program Requirements.
Merchant Digital Card-on-File (MDC)	A type of Click to Pay merchant checkout service that allows a cardholder to designate a payment credential as a merchant card-on-file for purchases with the merchant.
Onboarding and Integration	Onboarding and Integration define the means by which we grant Click to Pay System Participants credentials to interact with the Mastercard Click to Pay System. SRCi entities will utilize the Click to Pay Onboarding application, accessed via Mastercard Connect™, to register and onboard with the Mastercard Click to Pay System, and register their respective DSAs through a provided Registration API.
One Time Password (OTP)	A one time pass-code used for identity authentication
PCI/DSS Compliance	The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance security of Personally Identifiable Information (PII Data) and cardholder data. In general, the following PCI standards must be met in order for a retailer to be deemed compliant: they must maintain and test a secure network, they must map the flow of cardholder data, and they must protect cardholder data.

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person. 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 the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Personal Data Breach	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.
PII Data	PII Data refers to an industry standard of personally identifiable cardholder information.
Privacy and Data Protection Requirements	All applicable laws, rules, regulations, directives, and governmental requirements relating in any way to the privacy, confidentiality, security and protection of Personal Data, including, without limitation, (a) EUR Data Protection Law, (b) all U.S. state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the processing of individuals' Personal Data, including the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (California Civil Code §§ 1798.100 to 1798.199) ("CPRA"), Colorado Privacy Act (Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313) ("ColoPA"), the Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15) ("CPOMA"), the Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("UCPA"), and the Virginia Consumer Data Protection Act (Virginia Code Ann. §§ 59.1-575 to 59.1-585) ("VCDPA"); (c) the Gramm-Leach-Bliley Act; (d) applicable laws regulating unsolicited email communications; (e) applicable laws relating to security breach notifications; (f) applicable laws imposing minimum security requirements; (g) applicable laws requiring the secure disposal of records containing certain Personal Data; (h) applicable laws regulating banking secrecy and outsourcing requirements; (i) applicable laws regulating international data transfers and/or on-soil requirements; (j) applicable laws regulating incident reporting and data breach notification requirements, including guidelines and recommendations from the competent Regulators; (k) other similar applicable laws; (l) to the extent

	applicable, the Payment Card Industry Data Security Standards (PCI DSS), and (m) all applicable provisions of a party's written information security policies, procedures and guidelines.
Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated 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.
Processor	The entity which processes Personal Data on behalf of a Controller.
Push Provisioning	Push Provisioning is the ability for a consumer to provision their account number to a Token Requestor, starting their journey from their Issuer banking application or website: the account number is pushed from the Issuer's environment to the Token Requestor's environment. Push Provisioning is also known as "Issuer-initiated Digitization".
Requirement	A required act for the Click to Pay Program.
SLA	A Service Level Arrangement (SLA) is a an arrangement that establishes operational performance goals between a service provider and a customer. An SLA can provide two-way accountability, fact-based analysis, and reporting against predefined goals and measurements.
Software Development Kit (SDK)	An SDK is a set of tools and or guides that allow developers to create and develop software applications on a platform.

Term	Definition
SRCi	The Secure Remote Commerce Initiator (SRCi) interacts with the DPA and Click to Pay system to initiate and complete checkout. It also enables the discovery and selection of payment cards. Unless otherwise clearly indicated, means an SRCi participating in the Mastercard SRC Program.
Step-Up Authentication	Step-up authentication requires a user to authenticate at an increased authentication level (for example, via OTP) as required by the policy that protects the resource.
Token Service Providers (TSPs)	Token Service Providers (TSPs) are approved third party partners who help token requestors enable tokenized payments.
Tokenization	Tokenization, when applied to data security, is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value.
UI	User Interface

Description of the Processing Activities

This section describes the processing activities.

Subject-matter of the Processing Click to Pay Participating Issuer and Mastercard will Process Personal Data to provide the Service or as otherwise as described in the Mastercard Click to Pay Program Requirements.

Nature and Purpose of the Processing

- Click to Pay Participating Issuer Processes Personal Data for the purposes described in *EUR Data Protection Law, Roles of the Parties 1.1*.
- Mastercard Processes Personal Data for the purposes described in *EUR Data Protection Law, Roles of the Parties 1.2*.

Types of Personal Data Personal Data Processed in the context of the Service, in particular:

- Cardholder data such as First Name, Last Name, Address, Postal Code, Country, Email. Mobile Number, government ID
- Cardholder payment data such as PAN and Expiry
- Endpoint device characteristics such as device identifier, device name, device channel, IP Address

- Application level data such as Account Identifier, Session Identifier
- Any other Personal Data provided by Click to Pay Participating Issuer.

Categories of Data Subjects The Personal Data Processed in the context of the Services relate to cardholders.

Duration of the Processing Click to Pay Participating Issuer and Mastercard will Process Personal Data only for as long as necessary to provide the Service and to comply with applicable laws.

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.