



Mastercard Click to Pay Terms and Conditions

10 January 2024



SRCIS

Contents

- Audience..... 5
- Chapter 1: Overview and Definitions 6
- Chapter 2: Merchants and Merchant Service Providers..... 11
 - Merchants..... 13
 - Merchant Service Providers 13
 - Merchant Technology Providers 13
 - Merchant Rules..... 14
 - Merchant Obligations..... 14
 - Merchant Digital Card-on-File 15
 - Click to Pay Systems and Click to Pay System Program Standards..... 16
 - Use of Marks..... 16
 - Service Marks..... 16
 - Click to Pay System Marks..... 17
 - EMVCo, LLC Marks..... 17
 - Conflict with Law 17
 - Compliance..... 17
 - Examination and Audit..... 18
 - Grant of License 18
 - Merchant Must Display Click to Pay Trigger 18
 - Merchant Advertising..... 19
 - Service Marks..... 19
 - Click to Pay System Marks..... 19
 - EMVCo, LLC Marks..... 20
 - Merchant Marks, Product Descriptions and Images..... 20
 - Certain Operational and Functional Requirements..... 20
 - Specifications 20
 - Updates 20
 - Outages 21
 - CVV Data..... 21
 - Implementing Checkout Postback..... 21
 - Merchant Customer Service 21
 - Service Existing Network Requirements 22
 - PCI Compliance 22
 - Merchant Service Provider Agreement with Merchants..... 22
 - Merchant Service Provider Obligations 23
 - Privacy and Data Protection; Data Usage..... 23

Compliance.....	23
Safeguards.....	24
Security Incidents.....	24
Governmental Request for Personal Data.....	24
Malware Prevention.....	24
Subcontractors.....	25
Data Transfers.....	25
Merchant Use.....	25
Merchant Service Provider Use.....	26
Use by Mastercard.....	26
Provision and Use of Information.....	27
Obligation to Provide Information.....	27
Use of Mastercard Information.....	27
Limitation on the Use of Reporting.....	27
Confidential Information.....	28
Safeguard Card Account and Transaction Information.....	28
Integrity of Brand and Network.....	28
Export.....	28
Indemnification.....	29
Disclaimer.....	29
Limitation of Liability.....	29
Termination.....	30
Voluntary Termination.....	30
Suspension or Termination by Mastercard.....	30
Effect of Termination.....	31
Choice of Laws.....	31
Chapter 3: Global Variations.....	32
Organization of this Chapter.....	33
Available Tokenization Choices for Mastercard Transactions.....	33
Chapter 4: Europe Region Variations.....	34
Privacy and Data Protection – Europe.....	35
Definitions.....	35
Roles of the Parties.....	36
Obligations of the Parties.....	36
Obligations of Controllers.....	37
Obligations of Processors.....	37
Data Transfers.....	38
Data Disclosures.....	38
Data Protection and Security Audit.....	39

Applicable Law and Jurisdiction 39

Notices 40

Audience

These Mastercard Click to Pay Service Terms and Conditions are applicable to Merchants and Merchant Service Providers.

Chapter 1 Overview and Definitions

Each Merchant and Merchant Service Provider that uses the Service agrees to comply with the Service Standards, including these Service Terms and each applicable Click to Pay System Program Standards, in each case as they may be amended from time to time.

These Terms apply to all Merchant implementations, and govern the conduct of Merchants and Merchant Service Providers, and activities related to their use of the Service. Mastercard has the right in its sole discretion to interpret, amend, and enforce the Service Standards. Mastercard reserves the right to limit, suspend or terminate a Merchant's or Merchant Service Provider's use of the Service.

Definitions

The following terms shall have the meanings ascribed below.

"Ancillary Service" means any Service-related feature or service made available by Mastercard to Participants on a mandatory or optional basis.

"Branding Standards" means branding specifications, requirements and guidelines provided or made available by Mastercard from time to time with respect to a Merchant's or Merchant Service Provider's use of the Service.

"Card Data" means a cardholder's account number, expiration date and CVV Data.

"Click to Pay Profile" means an account or profile registered with an Click to Pay System.

"Click to Pay Standard" or "Click to Pay" means the EMV Click to Pay Technical Framework, version 1.0, and the EMV Click to Pay Specification, version 1.0, and other SRC Specifications (as defined therein), including all new versions and updates thereto.

"Click to Pay System" means each Click to Pay System (as defined in the Click to Pay Standard) supported by the Service.

"Click to Pay System Marks" means, with respect to each Click to Pay System, the names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks associated with such Click to Pay System.

"Click to Pay System Program Standards" means, with respect to each Click to Pay System, the applicable rules, standards, requirements, policies, guidelines and other documentation of such Click to Pay System and its Click to Pay Program (as such terms is defined under the Click to Pay Standard), as may be amended and updated from time to time by such Click to Pay System, relating to transactions supported by such Click to Pay System (or associated payment network) and facilitated by the Service under these Service Terms. Click to Pay System Program Standards may include, without limitation, relevant payment network operating rules, branding standards and guidelines, and transaction processing rules. As of the effective date of these Service Terms:

- The Mastercard Click to Pay Program Rules document is available at <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/mastercard-src-merchant-dpa-program-requirements.pdf>.

- The American Express Click to Pay System has not made available to the Service any separate document of Click to Pay-related rules or standards of Merchants and Merchant Service Providers.

Merchants are advised that with respect to each Click to Pay System, other applicable Click to Pay

©2020–2023 Mastercard. Proprietary. All rights reserved.

Mastercard Click to Pay Terms and Conditions • 10 Jan 2024

System Program Standards may be found in, without limitation, the payment network operating rules and standards of such Click to Pay System.

"CVV Data" means the three or four digit card security code, usually printed to right of the card number in the signature panel on the back of a payment card (for American Express Cards it is on the front printed above the card identification data).

"Data Subject" means an identified or identifiable natural person, user, or cardholder, who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

"EMVCo Reproduction Requirements" means the Click to Pay: Payment Icon Reproduction Requirements, version 1.0, as updated or amended by EMVCo, LLC, and in effect from time to time. As of October 1, 2019, the EMVCo Reproduction Requirements are available at <https://www.emvco.com/wp-content/uploads/2019/06/EMV-Click-to-Pay-Payment-Icon-Reproduction-Requirements-v1.0-June-2019.pdf>.

"Malware" means computer software, code or instructions that: (a) adversely affect the operation, security or integrity of a computing, telecommunications or other digital operating or processing system or environment, including without limitation, other programs, data, databases, computer libraries and computer and communications equipment, by altering, destroying, disrupting or inhibiting such operation, security or integrity; (b) without functional purpose, self-replicate without manual intervention; (c) purport to perform a useful function but which actually perform either a destructive or harmful function, or perform no useful function and utilize substantial computer, telecommunications or memory resources; or (d) without authorization collect and/or transmit to third parties any information or data; including such software, code or instructions commonly known as viruses, Trojans, logic bombs, worms and spyware.

"Mastercard" means either (i) Mastercard International Incorporated, or (ii) in certain regions or countries in which the Mastercard Rules define or otherwise contemplate that "Mastercard" or "Corporation" (as such terms are used in the Mastercard Rules) shall be a particular affiliate or subsidiary of Mastercard International Incorporated, such affiliate or subsidiary of Mastercard International Incorporated.

"Merchant" means, for the purpose of these Service Terms, a Merchant (as defined in the Standards), including a Merchant that accepts payment cards from other payment networks, that is participating in the Service.

"Merchant Account" means an account established via the Merchant Portal to allow a Merchant to access the resources needed to connect to the Service.

"Merchant Content" means any content provided or made available by Merchant in connection with the Service (including, without limitation, descriptions and images of products or services available for purchase in connection with the Service).

"Merchant Digital Card-on-file" is a type of merchant checkout Service that allows a cardholder to designate a payment credential as a merchant card-on-file for purchases with Merchant.

"Merchant Marks" means a Merchant's name, logo, URL, service name or trademarks as designated by the Merchant or the Merchant Service Provider(s) or Merchant Technology Provider.

"Merchant Portal" means an electronic connection through which a Merchant or Merchant Service Provider can manage its respective Merchant Account or Merchant Service Provider Account in connection with its use of the Service.

"Merchant Service Provider" means a Service Provider (as defined in the Mastercard Rules) providing Service-related services to a Merchant.

"Merchant Service Provider Account" means an account established via the Merchant Portal to allow a Merchant Service Provider to access the resources needed to enable a Merchant to display the Service Trigger.

"Merchant Specifications" means any technical and operational specifications and guides provided or made available by Mastercard from time to time with respect to a Merchant's use of the Service.

"Merchant Technology Provider" means a service provider that is not considered a Service Provider under the Mastercard Rules and provides Service-related services including technology services.

"Merchant Terms and Conditions" means the terms and conditions between Merchant and cardholder for Merchant Digital Card-on-file.

"Participant" means any or all (as the context may require) Merchant and/or Merchant Support Provider and/or Merchant Technology Provider.

"Personal Data" means any information relating to a Data Subject (including a Data Subject's name, address, e-mail, telephone number, business contact information, date of birth, Social Security Number, credit or debit card number, bank account number, primary account number or token, loyalty number, transaction history and any other unique identifier or one or more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity).

"Privacy and Data Protection Requirements" means 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, to the extent applicable (a) the EU General Data Protection Regulation 2016/679 ("EU GDPR") and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) and their respective national implementing legislations; the Swiss Federal Data Protection Act; the Monaco Data Protection Act; the UK Data Protection Act 2018 and UK GDPR (together "UK Data Protection Law"); and the Data Protection Acts of the European Economic Area ("EEA") countries, and any relevant national implementing legislation, as well as guidance and recommendations from the competent Regulators; (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.

"Process" or "Processing", when used in reference to information, means any operation or set of operations which is performed upon information, whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,

blocking, erasure or destruction of such data.

"Reports" means any report a Merchant or a Merchant Service Provider is required to provide to Mastercard, whether on a one-time or repeated basis, pertaining to its use of the Service.

"Service" means services (including all Ancillary Services) offered by Mastercard pursuant to these Service Terms, including support in connection with Click to Pay-based payment transactions facilitated by Click to Pay Systems and certain value-added services.

"Service Marks" means the names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks associated with the Service and the from time to time in Mastercard's sole and absolute discretion and made available for use by Merchants and Merchant Service Providers and other authorized entities. For avoidance of doubt, "Service Marks" do not include names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks of any Click to Pay System or EMVCo, LLC.

"Service Materials" means all materials made available by Mastercard to a Merchant or Merchant Service Provider from time to time that are relevant to that entity's use of the Service. These materials include, without limitation, these Service Terms, the Service Marks, the Service Trigger, and the Specifications.

"Service Provider Specifications" means any technical and operational specifications provided or made available by Mastercard from time to time with respect to a Merchant Service Provider's use of the Service.

"Service Standards" means these Service Terms, the Branding Standards (or any equivalent documentation made available by Mastercard from time to time) and all Service Materials, in each case as in effect and amended from time to time.

"Service Terms" means these Mastercard Click to Pay Service Terms and Conditions, as amended by Mastercard, and in effect, from time to time.

"Service Trigger" means technology provided by Mastercard for the Service, including but not limited to, software, application programming interfaces, software development kits, plug-ins, and any other Mastercard systems, technologies, specifications, and documentation made available by Mastercard in connection with the Service to enable the Service and to initiate one or more Click to Pay events (e.g., set-up, enrollment, binding, recognition, checkout events, and Merchant Digital Card-on-file as contemplated by the Click to Pay Standard). The Service Trigger includes the Service Marks (as required by Mastercard from time to time and described in the Service Materials), which indicates a Merchant's use of the Service.

"Specifications" means the Merchant Specifications and the Service Provider Specifications.

Interpretation

Except as otherwise expressly provided herein, the following rules shall apply: (a) the singular includes the plural and the plural includes the singular; (b) all references to the masculine gender shall include the feminine gender (and vice versa); (c) "include," "includes" and "including" are not limiting; (d) unless the context otherwise requires or unless otherwise provided herein, references to a particular agreement, instrument, document, law or regulation also refer to and include all renewals, extensions, modifications, amendments and restatements of such agreement, instrument, document, law or regulation; (e) words such as "hereunder," "hereto," "hereof," and "herein," and other words of like import shall, unless the context clearly indicates to the contrary, refer to the whole of these Service Terms and not to any particular chapter, subsection or clause hereof; and (h) the headings, captions, headers, footers and version numbers contained in these Service Terms are inserted for convenience only and shall not affect the meaning or interpretation of these Service Terms.

Chapter 2 Merchants and Merchant Service Providers

This section describes Merchants and Merchant Service Providers.

Merchants.....	13
Merchant Service Providers.....	13
Merchant Technology Providers	13
Merchant Rules.....	14
Merchant Obligations.....	14
Merchant Digital Card-on-File	15
Click to Pay Systems and Click to Pay System Program Standards.....	16
Use of Marks.....	16
Service Marks.....	16
Click to Pay System Marks.....	17
EMVCo, LLC Marks.....	17
Conflict with Law	17
Compliance.....	17
Examination and Audit.....	18
Grant of License	18
Merchant Must Display Click to Pay Trigger.....	18
Merchant Advertising	19
Service Marks.....	19
Click to Pay System Marks.....	19
EMVCo, LLC Marks.....	20
Merchant Marks, Product Descriptions and Images.....	20
Certain Operational and Functional Requirements	20
Specifications	20
Updates	20
Outages	21
CVV Data.....	21
Implementing Checkout Postback.....	21
Merchant Customer Service	21
Service Existing Network Requirements.....	22
PCI Compliance	22
Merchant Service Provider Agreement with Merchants.....	22
Merchant Service Provider Obligations.....	23
Privacy and Data Protection; Data Usage	23
Compliance.....	23

Safeguards	24
Security Incidents	24
Governmental Request for Personal Data	24
Malware Prevention	24
Subcontractors.....	25
Data Transfers	25
Merchant Use.....	25
Merchant Service Provider Use	26
Use by Mastercard.....	26
Provision and Use of Information.....	27
Obligation to Provide Information.....	27
Use of Mastercard Information	27
Limitation on the Use of Reporting	27
Confidential Information.....	28
Safeguard Card Account and Transaction Information.....	28
Integrity of Brand and Network.....	28
Export	28
Indemnification.....	29
Disclaimer	29
Limitation of Liability	29
Termination	30
Voluntary Termination	30
Suspension or Termination by Mastercard.....	30
Effect of Termination.....	31
Choice of Laws	31

Merchants

To use the Service and accept Click to Pay-based transactions through the Service, a Merchant must (a) accept Mastercard-branded payment cards, and (b) either (i) register by creating a Merchant Account, selecting the services it will receive, and agree to be bound by these Service Terms; or (ii) if accessing the Service via a Merchant Service Provider, agree to be bound by these Service Terms.

In addition, each Merchant (and each Merchant Support Provider) must meet any requirements of each Click to Pay System that facilitates Click to Pay transactions at Merchant through the Service.

Merchant Service Providers

Service-related services performed by any entity, which services directly or indirectly support or otherwise benefit a Merchant's use of the Service and regardless of whether such entity is or was registered with Mastercard as a Merchant Service Provider or whether the entity is itself a Customer (as defined under the Mastercard Rules), subjects the Merchant to the indemnification and other obligations as set forth in the Service Standards, including without limitation these Service Terms.

With respect to Mastercard-branded transactions, A Merchant Service Provider may use the Service and perform related services for Merchants only if (i) said Merchant Service Provider is registered with Mastercard as a Service Provider in accordance with the Mastercard Rules by the Acquirer on behalf of which it is providing services to the Merchant, and (ii) said Merchant Service Provider has been registered with Mastercard by the Merchant for such services. Each Merchant Service Provider must maintain their registration as a Merchant Service Provider in good standing with Mastercard while it is providing Service-related services. Additionally, any entity performing Service-related services must create a Merchant Service Provider account on the Merchant Portal and must continue to update registration and account information promptly. Merchants shall ensure that their Merchant Service Providers comply with their obligations hereunder.

Merchant Technology Providers

A Merchant must disclose to Mastercard, in the manner prescribed by Mastercard from time to time, the name and contact details of any Merchant Technology Provider that performs services in connection with Merchant's use of the Service during the Merchant registration process (or, if after, within ten (10) calendar days of such Merchant Technology Provider starting to provide said services by sending a revised version of the registration documents including that Merchant Technology Provider's information), as well as any other information reasonably required by Mastercard regarding such Merchant Technology Provider and/or the services it provides.

Merchant Rules

Each Merchant, Merchant Service Provider(s) and Merchant Technology Provider(s), at all times during its use of the Service, must comply with the Service Standards and applicable Click to Pay System Program Standards.

Additional information can be found in the Service Materials. Merchants are responsible for their Merchant Service Provider and Merchant Technology Providers' compliance with these Service Terms (and the Service Standards and Click to Pay System Program Standards, as applicable).

Merchant Obligations

Each Merchant must:

1. Notify its Acquirer in writing of its use of any Merchant Service Provider(s) in connection with its use of the Service.
2. Be eligible to register and use the Service and have the right, power, and ability to comply with these Service Terms and each applicable Click to Pay System Program Standards.
3. Provide to Mastercard, either directly or through its Merchant Service Provider, the name or business name under which it sell goods and services.
4. Ensure, either directly or through its Merchant Service Provider, that it and all payment transactions initiated by it will comply with all laws, rules, and regulations applicable to its business, including any applicable tax laws and regulations.
5. Accurately describe, in a privacy notice available on its website or other e-commerce applications, its use of Personal Data received in connection with its use of the Service.
6. Provide all necessary notices to and obtain all necessary consents from users as required by law and Privacy and Data Protection Requirements to transfer Personal Data to Mastercard for its use in connection with the Service pursuant to these Service Terms, including each Click to Pay System Program Standards, as applicable.
7. Not facilitate transactions that are prohibited by the applicable rules, standards, requirements, policies, guidelines of any Click to Pay System or payment network supported by the Service.
8. Not use the Service, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Service.
9. Have or obtain all rights, consents, licenses, permissions and releases, including all intellectual property rights, necessary to provide or make available the Merchant Content for Mastercard's use in connection with the Service.
10. Only use, and ensure that its Merchant Service Providers only use, Personal Data provided by Mastercard for purposes of using the Service as contemplated in these Service Terms.
11. Not, by performing its obligations hereunder, violate any other agreement to which it is a party; and
12. Provide Mastercard with, and update as necessary, the contact details of an authorized representative of Merchant to receive electronically all communications from Mastercard in connection with the Service.

13. For each transaction, after receiving payload from Click to Pay system, SRCl must initiate EMV 3DS Transaction Authentication in order to comply with PSD2 regulation (A requirement, applies to EU region).
14. When utilizing Merchant Digital Card-on-file:
 - a. Require cardholder to create an account with Merchant.
 - b. Provide appropriate notice to and obtain consent from cardholder in order to retrieve payment credential(s) from Click to Pay and for merchant to store credential(s) for Merchant Card on File prior to retrieving payment credential(s) from Click to Pay.
 - c. Be solely responsible for the Merchant Terms and Conditions, including, but not limited to obtaining cardholder consent to and acceptance of the Merchant Terms and Conditions and maintaining appropriate records of such cardholder consent and acceptance.
 - d. Obtain cardholders' consent to designate a payment credential, which may be in the form of Card Data or other unique identifier as a merchant card-on-file.
 - e. Obtain cardholders' consent to allow recurring payments to be made using the merchant card-on-file.
 - f. Limit use of Merchant Digital Card-on-file solely for use with Merchant.
 - g. Be solely responsible for such credential once received through Merchant Digital Card-on-file.
 - h. Be solely responsible for addressing and resolving cardholder inquiries relating Merchant Digital Card-on-file.
15. In addition, when utilizing credentials received through Merchant Digital Card-on-file for purposes of furnishing such credentials to alternative card-on-file solutions:
 - a. 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. For the avoidance of doubt such alternative card-on-file solution is separate from and not included as part of Merchant Digital Card-on-file.
 - b. Be solely responsible for merchant's use such alternative card-on-file solution.
16. Comply with other merchant requirements and obligations set forth in these Service Terms.

Merchant Digital Card-on-File

Merchant acknowledges and agrees that in the event Merchant enables Merchant Digital Card-on-file, Merchant may receive Card Data (for Mastercard branded cards) or other unique identifier (for non-Mastercard branded cards) as the payment credential to store on file.

Utilization of Merchant Card-on-file is separate from and does not restrict Merchant from utilizing a tokenized or other card-on-file solution that may be provided by Mastercard, for example Secure Card on File or M4M, other network or other third party, each subject to the applicable terms and conditions for such separate service.

With regard to non-Mastercard branded cards:

1. Merchant will receive 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.
2. Such unique identifier will not be updated in the event the original associated card is updated resulting in the need for the cardholder to potentially read such payment credential as a merchant card-on-file.

Click to Pay Systems and Click to Pay System Program Standards

As between each Merchant and the Service, Merchant has sole discretion to choose the particular payment brands (among those supported by the Service) that are accepted by the Merchant via the Service.

However, Merchant acknowledges that it may be subject to certain requirements of each payment brand under other agreements and standards relating to such brand, and the optionality provided by the Service and described in the foregoing sentence has no effect on Merchant's acceptance obligations (if any) under such agreements and/or standards.

The acceptance of each payment brand that is acceptable through the Service is facilitated by one or more third party Click to Pay Systems. The Service is made available to Merchant subject to the rights and obligations of Mastercard (solely in its capacity as provider of the Service) and Merchant under each Click to Pay System's respective Click to Pay System Program Standards.

With respect to each payment brand that Merchant accepts through the Service, Merchant is subject to, and must comply with, the applicable Click to Pay System Program Standards for such payment brand and applicable Click to Pay System. Merchant may be described as a "merchant", "digital payment application", "DPA" or other terms describing the roles and responsibilities of Merchant under such Click to Pay System Program Standards. Mastercard is not responsible for any breach or failure by Merchant to comply any Click to Pay System Program Standards. Merchant's breach of Click to Pay System Program Standards may result in certain consequences from (or with respect to) the applicable Click to Pay System or payment brand under the applicable Click to Pay System Program Standards or other applicable payment network rules, including, but not limited to, termination or suspension of Merchant's ability to use the Service to accept Click to Pay-based transactions of such Click to Pay System or payment brand.

Use of Marks

This section describes the use of marks.

Service Marks

Any use of the Service Marks by a Merchant, its Merchant Service Provider or Merchant Technology Provider, including in acceptance advertising, acceptance decals, or signs, must be in accordance with the Standards, including the Service Branding Requirements, which are incorporated into these Service Terms by reference.

A Merchant's, Merchant Service Provider's or Merchant Technology Provider's use or display of the Service Marks will terminate effective with the termination of the Merchant's use of the Service.

The use or display of any Service Marks does not give a Merchant, Merchant Service Provider or Merchant Technology Provider any ownership or interest in the Service Marks. All proprietary

rights and goodwill associated with the use of any Service Marks by Merchant, Merchant Service Provider or Merchant Technology Provider shall inure to the benefit of Mastercard.

Click to Pay System Marks

A Merchant's, Merchant Service Provider's or Merchant Technology Provider's right to use any Click to Pay System Marks in connection with their use of the Service is subject to the respective Click to Pay System Program Standards of each applicable Click to Pay System, subject to the Click to Pay Systems and Click to Pay System Program Standards Section of these Service Terms.

EMVCo, LLC Marks

The EMV® Click to Pay payment icon, consisting of a pentagon design oriented on its side with a stylized depiction of a fast forward symbol on the right, formed by a continuous line (the "EMVCo Click to Pay Icon"), is a trademark owned by and used with permission of EMVCo, LLC.

A Merchant's, Merchant Service Provider's or Merchant Technology Provider's right to use the EMVCo Click to Pay Icon in connection with their acceptance of Click to Pay transactions by a particular Click to Pay System is subject to Merchant's compliance with:

1. The EMVCo Reproduction Requirements.
2. The Click to Pay System Program Standards of each applicable Click to Pay System.
3. The Click to Pay Systems and Click to Pay System Program Standards Section of these Service Terms.

Conflict with Law

A Participant is not required to undertake any act as part of its use of the Service that is unambiguously prohibited by applicable law or regulation.

Compliance

Each Merchant, Merchant Service Provider and Merchant Technology Provider must fully cooperate with any effort by Mastercard and Mastercard's representatives to evaluate a Merchant's, Merchant Service Provider's or Merchant Technology Provider's compliance with the Service Standards, including these Service Terms.

In the event that Mastercard determines that a Merchant, Merchant Service Provider or Merchant Technology Provider is not complying or may not on an ongoing basis comply with the aforementioned requirements, Mastercard may require a Merchant, Merchant Service Provider or Merchant Technology Provider to take action and Mastercard itself may take action as Mastercard deems necessary or appropriate to address noncompliance with these Service Terms and to otherwise safeguard the integrity of the Service.

Examination and Audit

Mastercard reserves the right to conduct an audit or examination of any Merchant or Merchant Service Provider to ensure full compliance with the Service Standards.

Any such audit or examination is at the reasonable expense of the Merchant or Merchant Service Provider, and a copy of the audit or examination results must be provided promptly to Mastercard upon request. For the avoidance of doubt, should a Merchant Service Provider be unable or unwilling to cover the cost of such audit or examination, the audit or examination shall be at the responsible Merchant's expense. Mastercard shall not exercise this right more than once a year unless Mastercard has reason to believe that the Merchant or Merchant Service Provider does not materially comply with the Service Standards.

Grant of License

During the term of the Merchant's use of the Service, Mastercard grants (i) Merchant, and by its use of the Service Trigger the Merchant accepts, and (ii) Merchant Service Providers, a non-exclusive, non-transferable, non-sub licensable, royalty-free, revocable, worldwide license to use the Service Trigger and Service Marks (and other related designs, graphics, logos, page headers, button icons, scripts, and service names as may be designated by Mastercard from time to time, but for the avoidance of doubt not including any Click to Pay System Marks or the EMVCo Click to Pay Icon), solely (a) to identify that Click to Pay acceptance (using the Service) is available as a checkout method on its website or other e-commerce application, and (b) in accordance with Mastercard's most up-to-date Branding Standards (or any equivalent documentation made available by Mastercard from time to time).

The license shall remain in effect until the Merchant's and/or Merchant Service Provider's use of the Service is terminated in accordance with these Service Terms. The Merchant and Merchant Service Provider shall promptly cease use of the Service Marks and Service Trigger if their use of the Service has been suspended or terminated.

In addition, in connection with the acceptance of transactions supported by any Click to Pay System, Merchant's right to use any relevant Click to Pay System Marks and the EMVCo Click to Pay Icon may be set forth in the applicable Click to Pay System Program Standards.

Merchant Must Display Click to Pay Trigger

A Merchant or Merchant Service must prominently display the Service Trigger in accordance with the Service Standards and Specifications, including the Service Branding Requirements, wherever card or other payment options are presented to indicate that Service is a checkout option. Merchants must display the Click to Pay button at parity with other checkout solutions during the checkout funnel.

If the Service Trigger does not function or its functionality is materially impaired for causes attributable to Mastercard or its agents and contractors (and not due to Merchant), Merchant

shall notify Mastercard as soon as reasonably practicable, and allow Mastercard no less than forty-eight (48) hours to resolve such issue. During such time, Merchant shall not disable the Service Trigger. If following such forty-eight (48) hour period, Mastercard is not able to resolve the issue affecting the functionality of the Service Trigger, Merchant may disable the Service Trigger and/or remove it from the Merchant properties until Mastercard has resolved such issue(s). Upon receipt of notice from Mastercard that the issue has been resolved, Merchant shall re-enable the Service Trigger on the Merchant properties within forty-eight (48) hours of the receipt of notification thereof from Mastercard.

Merchant Advertising

A Merchant may use the Service Marks, Click to Pay System Marks and EMVCo Click to Pay Icon in advertising materials and/or to indicate acceptance of Click to Pay-based transactions subject to this Section.

Service Marks

A Merchant may use the Service Marks in advertising material and/or to indicate acceptance of Click to Pay-based transactions via the Service.

Other marks, symbols, logos, or combination thereof may appear in the same material or image with the Service Marks, if no other mark, symbol, or logo is more prominent or likely to cause confusion concerning the Merchant's use of the Service.

In marketing or referencing Service, the Merchant or its Merchant Service Providers will portray the Service accurately and fairly and not make any representations, warranties or guaranties inconsistent with any information provided by Mastercard. Except as expressly provided in the Branding Standards (or any equivalent documentation made available by Mastercard from time to time) or approved by Mastercard in writing, a Merchant or its Merchant Service Providers may not use any of the Service Marks in an offline promotion or other offline materials (e.g., in printed material, mailings or documentation) that they intend to distribute. The Merchant and its Merchant Service Providers shall not use the Service Marks in connection with any product or service that is not related to the Service, in any manner that is likely to cause confusion among users or in any manner that disparages or discredits Mastercard. All other trademarks not owned by Mastercard that appear in connection with the Service are the property of their respective owners, which may or may not be affiliated with, connected to, or sponsored by Mastercard.

Click to Pay System Marks

A Merchant's right to use any Click to Pay System Marks in advertising material and/or to indicate acceptance of Click to Pay-based transactions supported by the applicable Click to Pay

System (or payment network) is set forth in, and subject to, the Click to Pay System Program Standards of each applicable Click to Pay System.

EMVCo, LLC Marks

A Merchant's right to use the EMVCo Click to Pay Icon in advertising material and/or to indicate acceptance of Click to Pay-based transactions is set forth in, and subject to, (i) the EMVCo Reproduction Requirements, and (ii) the Click to Pay System Program Standards of each applicable Click to Pay System.

Merchant Marks, Product Descriptions and Images

Mastercard may use the Merchant Marks and the Merchant Content (i) as necessary to provide Service-related services, (ii) to identify the Merchant as an Click to Pay-accepting merchant and a customer of the Service including related educational, promotional or marketing materials.

Certain Operational and Functional Requirements

This section describes certain operational and functional requirements.

Specifications

Each Merchant and Merchant Service Provider must conduct activities related to their use of the Service in full compliance with all applicable laws and regulations.

Each Merchant and Merchant Service Provider must conduct all activity and otherwise operate in a manner that is financially sound and so as to avoid risk to Mastercard.

A Merchant and its Merchant Service Providers must comply with the Specifications. Mastercard reserves the right to update or modify the Specifications at any time.

Prior to a Merchant or its Merchant Service Providers making a website or other e-commerce application generally available for use with the Service, it must test each to ensure that it operates properly with the Specifications. A Merchant or its Merchant Service Providers must correct any material errors, defects or other non-compliance of which they become aware, including from review and test results provided by Mastercard, pursuant to the Merchant Must Display Click to Pay Trigger Section of these Service Terms.

Updates

Mastercard may make modifications, updates or upgrades to the Service or related Specifications.

Each Merchant and/or Merchant Service Provider must upgrade to the latest version of the Specifications within six (6) months from the release of such Specifications. Notwithstanding the foregoing, each Merchant will test and, if necessary, promptly modify its integration and/or any Service-connected websites or other e-commerce applications, at its own expense, to ensure continued Service acceptance using the then-current version of the Specifications and the Service. Except for reasons of security or to address an outage, neither Merchants nor their

Merchant Service Providers shall be required to make any changes to their system during the months of November and December. Mastercard retains the right to track each Merchant's and their Merchant Service Provider's implementation of the Specifications.

Outages

Each Merchant, or its Merchant Service Provider, shall notify Mastercard as soon as reasonably practicable of any outage and take any such remedial actions as are required to re-establish Service acceptance within 48 hours after the beginning of the outage.

Neither Merchant nor their Merchant Service Provider(s) shall impute the cause of the outage on Mastercard without Mastercard's prior written consent.

CVV Data

A Merchants and their Merchant Service Providers must not require a user to enter CVV Data in connection with a transaction initiated via the Service without the express written consent of Mastercard, except where such collection is specifically required by the Click to Pay Program System Program Standards or other payment network rules applicable to such transaction.

A Merchant and its Merchant Service Provider(s) must not store CVV Data at any time.

Implementing Checkout Postback

A Merchants and/or their Merchant Service Providers must implement checkout postback expressly as described in the Specifications without modification and shall apply it to every transaction conducted via the Service.

A Merchants and/or their Merchant Service Providers must communicate the result (success or failure) of the transaction conducted via the Service or any other information required pursuant to the most current Specifications. Abandoned transactions do not need to be reported.

Merchant Customer Service

A Merchant is solely responsible for all customer service relating to its website and other e-commerce application used in connection with the promotion or sale of goods or services; its business; the goods or services (including pricing, rebates, item information, availability, technical support, functionality and warranty) offered; order fulfillment (including shipping and handling); payment for goods or services; order cancellation by the Merchant or a user; returns, refunds and adjustments; and feedback concerning experiences with the Merchant's or its Merchant Service Provider(s)' personnel, policies or processes.

In performing customer service, a Merchant and its Merchant Service Provider(s) will always present themselves as a separate entity from Mastercard.

Service Existing Network Requirements

Use of the Service in no way relieves a Merchant or its Merchant Service Providers from its or their obligations under applicable payment networks' rules with regard to transaction processing or acceptance.

PCI Compliance

Merchants must at all times be, or instead Merchant Service Providers must ensure that all Merchants for which they are performing Service-related services are (if applicable), compliant with the Payment Card Industry Data Security Rules (PCI DSS) and the Payment Application Data Security Rules (PA DSS), as applicable.

Merchants and Merchant Service Providers must promptly provide Mastercard with documentation evidencing compliance with PCI DSS and/or PA DSS if requested by Mastercard. This compliance must be determined by a Qualified Security Assessor (QSA) when applicable. Merchant Service Providers must use only PCI compliant Merchant Service Providers in connection with the storage, or transmission of Card Data. A Merchant Service Provider must not store CVV Data at any time. For more information, please consult <https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html>.

Merchant Service Provider Agreement with Merchants

A Merchant Service Provider may only enable a Merchant to use the Service and become a Merchant if (i) it has entered into an agreement with such Merchant regarding the Service-related services, and (ii) it has been provided by each Merchant with all necessary power and authority to enable Service-related services for such Merchant.

In such agreement with each Merchant, the Merchant Service Provider must obligate such Merchant to be bound by these Service Terms, as applicable, and each Merchant must agree to be so bound. Such agreement must also include an indemnity substantially as set forth below, and such indemnity shall not be subject to any limitation of liability or other limitation or restriction.

"Merchant will indemnify and hold harmless Merchant Service Provider and its Merchant Service Providers (and its and their respective employees, directors, officers, shareholders, agents and representatives, acknowledging that Mastercard is one such Merchant Service Provider) from and against any and all claims, costs, losses, damages, judgments, tax assessments, penalties, interest, and expenses (including without limitation reasonable attorneys' fees) arising out of any claim, action, audit, investigation, inquiry, or other proceeding instituted by a person or entity that arises out of or relates to: (a) any actual or alleged breach of a Merchant's obligations set forth in the Service Terms, including without limitation any violation of Mastercard's policies; (b) any actual or alleged breach of a Merchant's obligations set forth in any Click to Pay System Program Standards; (c) a Merchant's use of the Service; (d) the actions

of any person (including any developer and/or administrator) or entity the Merchant authorizes to integrate with or access the services on their behalf; and (e) any Transaction initiated by a Merchant using payment information provided to the Merchant Support Provider by the services."

Pursuant to any applicable Click to Pay System Program Standards or other relevant payment network rules, a Merchant's receipt of Service-related services from or through a Merchant Service Provider, regardless of whether receives such services pursuant to an agreement with the Merchant Service Provider, may subject the Merchant Service Provider and the customer(s) of payment network or Click to Pay System by which such Merchant Service Provider is or should be registered with such payment network or Click to Pay System to the indemnification and other obligations as set forth in the applicable Click to Pay System Program Standards or other relevant payment network rules.

Merchant Service Provider Obligations

A Merchant Service Provider that is providing Service-related services to Merchants must:

1. Provide accurate information to Mastercard regarding the Merchants that are implemented to display the Service Trigger;
2. Provide and maintain at its cost any necessary items required for its own access, on behalf of Merchants, to Service;
3. Not use the Service, and shall ensure each Merchant does not to use the Service, in any manner that adversely affects the Service or that in any manner could damage, disable, overburden, threaten the security of or impair any of Mastercard's proprietary technology (including, without limitation, servers or networks); and
4. Comply and will continue to comply with the Service Standards and all applicable laws and regulations in connection with providing Service -related services to Merchants, and ensure each Merchant complies and will continue to comply with all Service Standards and applicable laws and regulations in connection with its access and use of the Service.

Privacy and Data Protection; Data Usage

This section describes data usage, privacy and data protection.

Compliance

Each Merchant shall, and shall ensure that all of their Merchant Service Providers, comply with Privacy and Data Protection Requirements in connection with their use of the Service.

Each Merchant shall be responsible for filing notifications to and/or obtaining approvals from competent regulators as legally required under applicable Privacy and Data Protection Requirements.

Safeguards

Each Merchant shall, and shall ensure that all of their Merchant Service Providers, maintain a comprehensive written information security program that complies with all Privacy and Data Protection Requirements and includes technical, physical, and administrative/organizational safeguards designed to (a) ensure the security and confidentiality of Personal Data, (b) protect against any anticipated threats or hazards to the security and integrity of Personal Data, (c) protect against any actual or suspected unauthorized Processing, loss, or acquisition of any Personal Data (in each case, relating to Personal Data processed through a Merchant's integration with the Service, a "Merchant Security Incident"), (d) ensure the proper disposal of Personal Data, and (e) regularly test or otherwise monitor the effectiveness of the safeguards.

Security Incidents

Except to the extent prohibited by applicable law, Merchant shall inform the other in writing, in accordance with the account data compromise event procedures set forth in the Mastercard Rules, in a commercially reasonable timeframe upon discovery of any Merchant Security Incident and in particular of (i) any incident or 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; and (ii) any known security issue pertaining to the Service Express program that may result in such incidents.

Each Merchant shall be solely responsible for any notices to Data Subjects as a result of any Merchant Security Incident, as and to the extent required by applicable Privacy and Data Protection Requirements.

Each participating Customer and Mastercard shall reasonably cooperate with each other in all matters relating to Merchant Security Incidents.

Governmental Request for Personal Data

Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, each of Mastercard and each Merchant shall inform each other in writing within forty-eight (48) hours of the request 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 the Service that relates to the Merchant's commerce platform.

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.

Malware Prevention

Mastercard and each Merchant will take commercially reasonable diligent measures to ensure that Malware is not coded or introduced into its respective systems interacting with the Service or Mastercard's or a Merchant's systems interacting therewith.

Mastercard and each Merchant will each continue to review, analyze and implement improvements to and upgrades of its Malware prevention and correction programs and processes that are commercially reasonable and consistent with the then current information technology industry's standards. If Malware is found to have been introduced into the Service or Mastercard's or Merchant's systems interacting therewith, Mastercard and the affected

Merchant(s) will cooperate and use commercially reasonable efforts to promptly communicate, and diligently work to remedy the effects of, the Malware.

Subcontractors

Mastercard and each Merchant shall remain liable towards the others for the Processing of Personal Data carried out by its respective subcontractors in connection with the Service and shall bear responsibility for the correct fulfillment of their respective obligations.

Mastercard and each Merchant are authorized to use subcontractors and shall impose on its subcontractors at least the same level of data protection including the same confidentiality a security obligations as required under this Section and shall prohibit its subcontractors to Process Personal Data other than as instructed.

In addition to the terms and conditions set forth in these Mastercard Click to Pay Service Terms and Conditions, including without limitation the applicable Click to Pay System Program Standards, the following shall apply with respect to Merchant's or Merchant Service Provider's use of the Plug-in Model. Merchant or Merchant Service Provider acknowledge and agree that Mastercard may use third party subcontractors and may use and disclose (i) Merchant or Merchant Service Provider data for the purpose of managing risk, franchise quality, and compliance purposes, and (ii) Merchant, Merchant Service Provider, and cardholder data as required for enabling and otherwise processing Click to Pay-based transactions through the Service. For purposes of this Section, "Plug-in Model" means the method of accessing the Service using an independent software component (e.g. a plug-in) made available by Mastercard directly or through a third party that connects to an application programming interface or software developer kit to access the Service.

Data Transfers

Personal Data processed in connection with the Service shall be transferred to and stored by Mastercard in the United States, in accordance with applicable Privacy and Data Protection Requirements.

To the extent Mastercard is receiving Personal Data of residents of the European Economic Area or Switzerland, Mastercard will cause such data to be transferred to the United States pursuant to Mastercard's Binding Corporate Rules, including as defined in [Privacy and Data Protection – Europe](#) of these Service Terms.

Merchant Use

Except as otherwise contemplated under these Service Terms, unless a Merchant or its Merchant Service Provider provides notice and receives the consent of the user, it may not retrieve, retain, track, monitor, store or otherwise use Personal Data regarding the user for any purpose other than to process the payment transaction facilitated by its use of the Service.

Absent notice and/or consent of the user and to the extent that Personal Data resides on a Merchant's or its Merchant Service Provider's systems or other storage locations: (a) Merchant may use the Personal Data only for the purpose of processing the related transaction; and (b) all Personal Data and other information provided to a Merchant or its Merchant Service Providers by Mastercard in relationship to use of the Service will remain the property of Mastercard.

Notwithstanding the foregoing, Merchants may not retain, track, monitor, store or otherwise

Merchants and Merchant Service Providers

use Personal Data regarding the user for the purpose of, or in any way that results in, bypassing the Service except where permitted by Mastercard in the Specifications or otherwise.

If a Merchant engages a third-party developer and/or administrator in implementing and/or managing its use of the Service and such third-party obtains from Mastercard any Personal Data, the third-party may not use any such Personal Data other than for the purpose of implementing and/or managing the Merchant's use of the Service. The third-party must destroy or otherwise cease to retain any Personal Data as soon as it is no longer necessary to fulfill the purpose for which it was received. The Merchant shall ensure that its employees, agents and sub-contractors who may receive or have access to Personal Data are aware of the obligations specified under these Service Terms, and agree to comply with such obligations.

Merchant Service Provider Use

A Merchant Service Provider may only retrieve, retain, track, monitor, store or otherwise use Personal Data in accordance with its provision of Service-related services to a Merchant, and in compliance with these Service Terms (including, for the avoidance of doubt, in accordance with applicable law, all applicable privacy policies including those of a Merchant (as defined in the Rules), as applicable, respecting such Personal Data, and the Mastercard Rules and/or other networks' rules, as applicable).

A Merchant Service Provider agrees that it will not use nor disclose Personal Data, or provide it to any party (other than Mastercard in accordance with the terms hereof) for any purpose other than to support its provision of Service-related services to a Merchant or Customer in accordance with the terms hereof. If a Merchant Service Provider engages a third-party developer and/or administrator in performing Service-related services, including implementing and/or managing the Service Trigger on a Merchant website or other Merchant Service Provider applications, and, in connection therewith, obtains from Mastercard any Personal Data regarding such developer and/or administrator, unless the Merchant Service Provider receives consent from such developer and/or administrator and provides any notices required in connection with the use thereof, a Merchant Service Provider may not use any such Personal Data other than for the purpose for which it was received.

Use by Mastercard

A Merchant must provide notice and obtain consent from all users necessary to ensure that, at a minimum, Mastercard has the right to use and disclose Personal Data it receives from a Merchant or its Merchant Service Provider for the following purposes:

1. Create and manage an online account, provide Service-related products and services, respond to user inquiries and provide customer service to respond to inquiries made by users;
2. Protect against and prevent fraud, unauthorized transactions, claims and other liabilities, and manage risk exposure and franchise quality;
3. Operate, evaluate, audit and improve the Service (including by developing new product features and services; managing communications; determining the effectiveness of advertising; analyzing Service-related products, services and websites; facilitating the functionality of our websites; and performing accounting, auditing, billing, reconciliation and collection activities);
4. Perform data analyses (including anonymization of Personal Data) to determine, among other measurements, business performance, number of registrants, channels, transaction spend and site performance, and creation of analytical models;
5. For preparing and furnishing compilations, analyses and other reports of aggregated information in connection with the Service;
6. Enforce these Service Terms;
7. Comply with applicable legal requirements and industry standards and Mastercard policies; and
8. Perform auditing, research and analysis in order to maintain, protect and improve our services.

In the event that Mastercard provides Personal Data to a Merchant and/or its Merchant Service Providers relating to the Service, the Merchant and its Merchant Service Providers shall only use such Personal Data for the purposes permitted by these Service Terms and applicable Privacy and Data Protection Requirements.

Provision and Use of Information

This section describes provision and use of information.

Obligation to Provide Information

Upon request by Mastercard, and subject to applicable law and regulation, a Merchant or Merchant Service Provider must provide Reports to Mastercard, or to Mastercard's designee; provided, compliance with the foregoing obligation does not require a Merchant or Merchant Service Provider to furnish any information the disclosure of which, in the written opinion of Merchant's or Merchant Service Provider's legal counsel, as applicable, is likely to create a significant potential legal risk to the Merchant and Merchant Service Provider.

To the extent that there is an obligation to provide a Report to Mastercard that the Merchant or Merchant Service Provider deems to disclose proprietary information of the Merchant, such information will be treated by Mastercard with the degree of care deemed appropriate by Mastercard to maintain its confidentiality.

Use of Mastercard Information

Mastercard is not responsible and disclaims any responsibility for the accuracy, completeness, or timeliness of any information disclosed by Mastercard to a Merchant or a Merchant Service Provider.

Mastercard makes no warranty, express or implied, including any warranty of merchantability or fitness for any particular purpose with respect to any information disclosed by or on behalf of Mastercard to any Merchant or a Merchant Service Provider.

Limitation on the Use of Reporting

Mastercard may use or disclose the Reports furnished by a Merchant or Merchant Service Provider to the extent allowed by applicable law and as specified herein, including protecting against and preventing fraud, unauthorized transactions, claims and other liabilities; managing risk exposure and franchise quality; operating, evaluating and improving our business (including by developing new products and services or removing current products or features; managing our communications; determining the effectiveness of our advertising; analyzing our products, services and websites; facilitating the functionality of the Service; and performing accounting, auditing, billing, reconciliation and collection activities); monitoring the use of and improve our interactive assets; and perform data analyses (including anonymization of Personal Data) to determine, among other measurements, business performance, number of registrants, channels, transaction spend and performance of the Service.

Confidential Information

A Merchant or a Merchant Service Provider may receive information (whether written, oral, electronic, or otherwise) as part of use of the Service relating to Mastercard or to the Service that is not freely available to the general public ("Confidential Information").

Each Merchant and Merchant Service Provider agrees that: (a) all Confidential Information will remain exclusive property of Mastercard, unless otherwise agreed to by the parties in writing; (b) it will use Confidential Information only as is necessary for its use of the Service; and (c) it will not otherwise disclose Confidential Information to any individual, company, or other third party.

Safeguard Card Account and Transaction Information

Each Merchant and each Merchant Service Provider that may be afforded access to Transaction or Personal Data, or both must safeguard and use or permit use of such information in accordance with the Standards.

A Merchant or a Merchant Service Provider may also have access to transaction or card account information from other payment networks, and must use such information in accordance with those payment network rules.

Integrity of Brand and Network

In connection with the Service, Merchant or a Merchant Service Provider must not directly or indirectly engage in or facilitate any action that is illegal, or that, in the opinion of Mastercard and whether or not addressed elsewhere in the Service Standards, damages or may damage the goodwill or reputation of Mastercard or of any Service Mark, and the Merchant or the Merchant Service Provider will promptly cease engaging in or facilitating such action upon request of Mastercard.

In connection with the Service, a Merchant or a Merchant Service Provider may be required to provide notice, obtain consent from users, or file any necessary documents with the local regulatory authorities as required by applicable law in connection with fraud solutions implemented by Mastercard designed to protect the integrity of the brand and/or Service. Without limiting the generality of the foregoing, specific obligations will be defined in the Service Materials.

Export

Merchants and Merchant Service Providers shall not import or export any of the Service Materials without first obtaining Mastercard's written approval.

If so permitted to import or export Service Materials, then Merchants and Merchant Service Providers shall comply with all foreign and U.S. export and import regulations applicable with respect to the Service Materials.

Indemnification

The Merchant and Merchant Service Providers will indemnify and hold harmless Mastercard and its Affiliates (and its and their respective employees, directors, officers, shareholders, agents and representatives) from and against any and all claims, costs, losses, damages, judgments, tax assessments, penalties, interest, and expenses (including without limitation reasonable attorneys' fees) arising out of any claim, action, audit, investigation, inquiry, or other proceeding instituted by a person or entity that arises out of or relates to: (a) any actual or alleged breach of the Merchant's and its Merchant Service Providers' obligations set forth in these Service Terms, including without limitation any violation of Mastercard's policies; (b) any actual or alleged breach of the Merchant's, or its Merchant Service Providers' or Merchant Technical Providers', obligations set forth in any Click to Pay System Program Standards, (c) wrongful or improper use of the Service; (d) the actions of any person (including any developer and/or administrator) or entity authorized by the Merchant or Merchant Service Provider to integrate with or access the Service on the Merchant's behalf; (e) any actual or alleged infringement, violation, or misappropriation of any intellectual property right, proprietary right or privacy right based upon any of the Merchant Marks, Merchant Content and/or equipment, processes, and other resources used by Merchant or others on its behalf in connection with the Service; (f) any dispute with a user relating to any product or service made available for purchase by Merchant in connection with the Service; (g) any personal injury, product liability or property damage related to any product or service made available for purchase by Merchant in connection with the Service; and (h) any payment card transaction initiated by the Merchant, or by a Merchant Service Provider on behalf of a Merchant, using payment information provided by the Service.

Disclaimer

THE SERVICE AND SERVICE MATERIALS ARE PROVIDED ON AN "AS IS" BASIS WITHOUT ANY WARRANTY WHATSOEVER.

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, MASTERCARD MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE SERVICE, THE SERVICE MATERIALS OR ANY ANCILLARY SERVICE INCLUDING WITHOUT LIMITATION: (A) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, OR NON-INFRINGEMENT; (B) THAT THE SERVICE MATERIALS, THE Service, OR ANY APPLICATION WILL MEET MERCHANT'S REQUIREMENTS, WILL ALWAYS BE AVAILABLE, ACCESSIBLE, UNINTERRUPTED, TIMELY, SECURE, FREE OF BUGS, VIRUSES, OPERATE WITHOUT ERROR OR OTHER DEFECTS, OR WILL CONTAIN ANY PARTICULAR FEATURES OR FUNCTIONALITY; OR (C) ANY IMPLIED WARRANTY ARISING FROM COURSE OF DEALING OR TRADE USAGE.

Limitation of Liability

TO THE EXTENT PERMITTED BY APPLICABLE LAW, MASTERCARD AND ITS AFFILIATES (AND MASTERCARD'S AND ITS AFFILIATES' RESPECTIVE EMPLOYEES, DIRECTORS, OFFICERS,

SHAREHOLDERS, AGENTS AND REPRESENTATIVES) WILL NOT BE LIABLE TO ANY MERCHANT OR MERCHANT SERVICE PROVIDER THAT PARTICIPATES IN THE Service OR TO ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE Service (INCLUDING THE INABILITY TO USE THE Service), THESE SERVICE TERMS, THE SERVICE MATERIALS, ANY APPLICATION, MERCHANT MARKS OR MERCHANT CONTENT, ANY ANCILLARY SERVICE, OR ANY SERVICES OR GOODS PURCHASED OR TRANSACTIONS ENTERED INTO THROUGH THE SERVICE.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL THE AGGREGATE LIABILITY OF MASTERCARD OR ITS AFFILIATES (AND MASTERCARD'S AND ITS AFFILIATES' RESPECTIVE EMPLOYEES, DIRECTORS, AGENTS AND REPRESENTATIVES) ARISING OUT OF OR IN CONNECTION WITH THE PROGRAM OR THE TRANSACTIONS CONTEMPLATED HEREBY, TO ANY MERCHANT THAT PARTICIPATES IN THE SERVICE OR TO ANY THIRD PARTY, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE, PRODUCT LIABILITY OR OTHER THEORY) OR OTHERWISE, EXCEED ONE THOUSAND (\$1,000) DOLLARS.

Termination

This section describes termination.

Voluntary Termination

A Merchant or a Merchant Service Provider may terminate its use of the Service by closing its Merchant Account or its Merchant Service Provider Account, respectively, at any time unless agreed otherwise expressly in writing.

Suspension or Termination by Mastercard

Mastercard may terminate a Merchant or a Merchant Service Provider's use of the Service and close its Merchant Account or Merchant Service Provider Account, respectively, at any time for any reason or for no reason, in its sole discretion, without any prior notice to the Merchant or Merchant Service Provider.

Without limiting the foregoing, Mastercard may suspend the participation of Merchant or Merchant Service Provider and access to its Merchant Account or Merchant Service Provider Account, respectively, if in its sole discretion the Merchant or Merchant Service Provider has violated the terms of these Service Terms (including any Standards), (b) the Merchant or Merchant Support Provider poses an unacceptable fraud risk to Mastercard or its Customers (as defined in the Mastercard Rules), or (c) the Merchant or Merchant Service Provider provides false, incomplete, inaccurate, or misleading information (including, without limitation, any registration information) or otherwise engage in fraudulent or illegal conduct. In addition, Mastercard may suspend and/or terminate a Merchant Service Provider's right to provide Service-related services to a Merchant at any time for any reason or no reason, in its sole discretion, subject to Mastercard providing notice to a Merchant Service Provider of such suspension. The Merchant Service Provider must, upon receipt of such notice, immediately terminate Service-related services to and for each such Merchant listed in such notice.

Effect of Termination

Upon termination of a Merchant or Merchant Service Provider's use of the Service, Mastercard will cease providing any access to the Service to the Merchant or Merchant Service Provider, respectively, and all Merchants who receive the access to the Service through the Merchant Service Provider, and the Merchant Service Provider and each Merchant's rights to access, use the Service (and any other rights) shall immediately cease.

WITHOUT LIMITING THIS SECTION, MASTERCARD WILL NOT BE LIABLE TO THE MERCHANT SERVICE PROVIDER OR ANY MERCHANT FOR ANY TERMINATION OR SUSPENSION OF ACCESS TO THE SERVICE, WHETHER UPON TERMINATION OF THE MERCHANT SERVICE PROVIDER'S PARTICIPATION THE SERVICE OR TERMINATION WITH RESPECT TO A PARTICULAR MERCHANT, INCLUDING WITHOUT LIMITATION FOR COMPENSATION, REIMBURSEMENT, OR DAMAGES ON ACCOUNT OF THE LOSS OF PROSPECTIVE PROFITS, ANTICIPATED SALES, GOODWILL, OR ON ACCOUNT OF EXPENDITURES, INVESTMENTS, OR COMMITMENTS IN CONNECTION WITH THE MERCHANT SERVICE PROVIDER OR A MERCHANT'S USE OF THE SERVICE.

Choice of Laws

The substantive laws of the State of New York govern all disputes involving Mastercard, the Service Standards, and/or the Merchant's or Merchant Service Provider's use of the Service without regard to conflicts of law provision or rule that would cause the application of the laws of any jurisdiction other than the State of New York.

Any action initiated by a Merchant or Merchant Service Provider regarding and/or involving Mastercard, the Service Standards and/or any Merchant or Merchant Service Provider must be brought only in the United States District Court for the Southern District of New York or the New York Supreme Court for the County of Westchester, and any Merchant or Merchant Service Provider involved in an action hereby submits to the jurisdiction of such courts and waives any claim of lack of personal jurisdiction, improper venue, and forum non conveniens.

Each Merchant and Merchant Service Provider agrees that the Service Standards are construed under, and governed by, the substantive laws of the State of New York without regard to conflicts of law provision or rule that would cause the application of the laws of any jurisdiction other than the State of New York.

Chapter 3 Global Variations

This section describes the global variations.

Organization of this Chapter.....	33
Available Tokenization Choices for Mastercard Transactions.....	33

Organization of this Chapter

The Standards in this Chapter 3 are variances and additions to the global Service Terms in Chapters 1 to 2, and apply to globally to all regions.

Refer to Appendix A of the Mastercard Rules for the United States Region geographic listing.

Available Tokenization Choices for Mastercard Transactions

A Merchant (whether directly or through Merchant Service Providers) may tokenize transactions through one of the following Mastercard-enabled tokenization models:

1. **Digital Secure Remote Payment (DSRP):** Mastercard generates a unique cryptogram associated with the token for each DSRP transaction.
2. **Dynamic Token Verification Code:** Mastercard generates a unique card validation code 2 (CVC 2) value and expiration date for each Dynamic Token Verification Code tokenized transaction.

Chapter 4 Europe Region Variations

This section describes the variations for the Europe region.

Privacy and Data Protection – Europe	35
Definitions.....	35
Roles of the Parties	36
Obligations of the Parties	36
Obligations of Controllers	37
Obligations of Processors.....	37
Data Transfers	38
Data Disclosures.....	38
Data Protection and Security Audit	39
Applicable Law and Jurisdiction.....	39

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 Service (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 Mastercard Click to Pay Terms and Conditions.

This section supplements the privacy and data protection terms contained in Chapter 2 [Privacy and Data Protection](#) of these Mastercard Click to Pay Terms and Conditions 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.

Definitions

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

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 EEA countries (as amended and replaced from time to time).

Europe means the European Economic Area, Switzerland, Monaco, and the United Kingdom.

Mastercard BCRs mean 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>.

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.

Processor means the entity which Processes Personal Data on behalf of a Controller.

Sub-Processor means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

Roles of the Parties

The parties acknowledge and confirm that:

Participating Merchants are Controllers and Mastercard, acting as an SCRI, is a Processor of the Merchant for (a) the distribution of Click to Pay code and (b) the management of Click to Pay API integration with the Mastercard SRC System. For the avoidance of doubt, Mastercard is a Controller for the Processing of Personal Data for the purpose of offering the Mastercard SRC System and Digital Card Facilitator Service to Click to Pay users.

Notwithstanding the above, Merchants acknowledge and agree that Mastercard, acting as an SCRI, may Process Personal Data for any purpose listed in Section *Privacy and Data Protection; Data Usage*, paragraph *Use by Mastercard* (refer to [Use by Mastercard](#)) of these Service Terms and in Section 3.10 of the Mastercard Rules, to the extent they apply, including internal research, fraud, security and risk management.

Merchant Service Providers and Merchant Technology Providers 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 Service; (b) are authorized by such Merchants to receive Personal Data from Click to Pay users or Mastercard via of the Service and Process that Personal Data on behalf of such Merchants. In addition, Merchant Service Providers, as Processors of Merchants, represent and warrant that they (b) received a mandate from such Merchants to enter into these Service Terms on behalf of such Merchants; and are authorized by such Merchants to enrol them into the Service or otherwise facilitate Merchants using the Service.

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

Obligations of the Parties

Each party must comply with applicable EU Data Protection Law when Processing Personal Data. Each party will:

(i) cooperate with the other party to fulfil 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 these Service Terms; 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, as applicable, parties 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 Service Terms, including the Processing for which Mastercard is a Controller.

Obligations of Controllers

Each party represents and warrants that, when it acts as a Controller, it will:

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

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

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).

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 Controller's Processor in which case the Controller is not required to inform Mastercard of such requests and Controller will be solely responsible for responding to such requests in accordance with EU Data Protection Law.

Obligations of Processors

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

Only Processes Personal Data in accordance with the Controller's lawful written instructions and not for any other purposes than those specified in these Service Terms, the Mastercard Rules, or as otherwise agreed by the parties in writing.

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

Cooperates with the Controller to fulfil the Controller'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 Controller's own obligations and where applicable to help the Controller in complying with its Personal Data Breach notification obligations and conducting data protection impact assessments or prior consultation with supervisory authorities.

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

Notifies the Controller when local laws prevent Mastercard (1) from fulfilling its obligations under this Section or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by this Section or the Mastercard BCRs, and (2) from complying with the instructions received from the Controller via this Section, 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 Controller is responsible for notifying its competent supervisory authority as applicable and required under EU Data Protection Law.

When Mastercard Click to Pay Terms and Conditions expire or terminate or upon a request to delete or return Personal Data by the Controller, Mastercard, in its role as Processor, will, at the choice of the Controller, delete, anonymize, or return all the Personal Data to the Controller, 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).

Data Transfers

In relation to its Processing of Personal Data in the context of the Service, 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 Service.

Data Disclosures

The parties represent and warrant that they will only disclose Personal Data Processed in the context of the Service 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 Mastercard Click to Pay Terms and Conditions.

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

When Mastercard acts as a Processor, Controllers give a general authorization to Mastercard to Process and sub-Process Personal Data to internal and external Sub-Processors in connection with the Service 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:

- Binds its internal Sub-Processors to respect Mastercard BCRs and to comply with the Controller's instructions.
- 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 Controller's instructions and with the same obligations as are imposed on Mastercard by this Section and the Mastercard BCRs, including sub-Processing and audit requirements set forth in Mastercard BCRs.
- Remains liable to the Controller for the performance of its Sub-Processor's obligations.

- Commits to provide a list of Sub-Processors to the Controller upon request.
- Will inform the Controller of any addition or replacement of a Sub-Processor in a timely fashion so as to give the Controller an opportunity to object to the change or to terminate its registration for the Service before the Personal Data is communicated to the new Sub-Processor, except where the Service cannot be provided without the involvement of a specific Sub-Processor.

Data Protection and Security Audit

Each party commits to conduct audits on a regular basis to control compliance with EU Data Protection Law, including the security measures provided under these Mastercard Click to Pay Terms and Conditions, 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 Section, 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.

When Mastercard acts as a Processor, Mastercard agrees to cooperate and within reasonable time provide the Controller with: (a) a summary of the audit reports demonstrating Mastercard's compliance with EU Data Protection Law obligations under this Section 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 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 Controller the result of the audit of its data protection compliance program.

Applicable Law and Jurisdiction

The parties agree that this Section 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.

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. 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.

EMV® is a registered trademark of EMVCo LLC in the United States and other countries. For more information, see <http://www.emvco.com>.

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.

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 Technical Resource Center (TRC). Go to the Rules collection of the References section for centralized information.