
# Masterpass Operating Rules

25 May 2018

MPOR

# Audience

These *Masterpass Operating Rules* are applicable to Customers, Customer Service Providers, Merchants and Merchant Service Providers.

# Summary of Changes, 25 May 2018

This document reflects changes associated with the 25 May 2018 publication. To locate these changes online, click the hyperlinks in the following table.

| Description of Change | Where to Look |
|---|---|
| Revised the 2.18.1 Compliance section. | 2.18.1 Compliance |
| Revised the 2.18.3 Security Incidents section. | 2.18.3 Security Incidents |
| Revised the 2.18.7 Data Transfers section | 2.18.7 Data Transfers |
| Revised the 2.19 Mastercard's Use of Personal Data section. | 2.19 Mastercard's Use of Personal Data |
| Revised the 3.21.7 Data Transfers section. | 3.21.7 Data Transfers |
| **SUBSECTION B Data Protection – Mastercard-Hosted Wallet: Europe Region only** | |
| Revised B.1 Definitions. | B.1 Definitions |
| Revised B.2 Processing of Personal Data. | B.2 Processing of Personal Data |
| Renamed B.3 Data Subject Notice and Consent to B.3 Data Transfers and revised the section | B.3 Data Transfers |
| Renamed B.4 Data Subjects' Requests to B.4 Data Disclosures and revised the section. | B.4 Data Disclosures |
| Renamed B.5 Integrity of Personal Data to B.5 Security of the Processing; Confidentiality; and Personal Data Breach and revised the section. | B.5 Security of the Processing; Confidentiality; and Personal Data Breach |
| Renamed B.6 Security Requirements to B.6 Data Protection and Security Audit and revised the section. | B.6 Data Protection and Security Audit |
| Renamed B.7 Data Transfer Requirements to B.7 Liability and revised the section. | B.7 Liability |
| Added the B.8 Applicable Law and Jurisdiction section. | B.8 Applicable Law and Jurisdiction |
| Renamed B.8 Public Authority's or Regulator's Requests to B.9 Public Authority's or Regulator's Requests and revised the section. | B.9 Public Authority's or Regulator's Requests |
| **SUBSECTION C Data Protection – Partner-Hosted Wallet: Europe Region only** | |
| Revised C.1 Definitions. | C.1 Definitions |
| Renamed C.2 Processing of Personal Data to C.2 Roles of the Parties and revised the section. | C.2 Roles of the Parties |
| Renamed C.3 Data Subject Notice and Consent to C.3 Obligations of Customer and revised the section. | C.3 Obligations of Customer |

| Description of Change | Where to Look |
|---|---|
| Renamed C.4 Data Subjects' Requests to C.4 Obligations of Mastercard and revised the section. | C.4 Obligations of Mastercard |
| Renamed C.5 Security to C.5 Data Transfers and revised the section. | C.5 Data Transfers |
| Renamed C.6 Data Transfer and Storage to C.6 Sub-Processing and revised the section. | C.6 Sub-Processing |
| Added the C.7 Security of the Processing; Confidentiality; and Personal Data Breach section | C.7 Security of the Processing; Confidentiality; and Personal Data Breach |
| Added the C.8 Data Protection Audit section | C.8 Data Protection Audit |
| Added the C.9 Liability Towards Data Subjects section | C.9 Liability Towards Data Subjects |
| Added the C.10 Applicable Law and Jurisdiction section | C.10 Applicable Law and Jurisdiction |
| **SUBSECTION D Data Protection – Merchant Rules: Europe Region Only** | |
| Added SUBSECTION D Data Protection – Merchant Rules: Europe Region Only containing:<br>• D.1 Definitions<br>• D.2 Processing of Personal Data<br>• D.3 Data Transfers<br>• D.4 Data Disclosures<br>• D.5 Security of the Processing; Confidentiality; and Personal Data Breach<br>• D.6 Data Protection and Security Audit<br>• D.7 Liability<br>• D.8 Applicable Law and Jurisdiction | SUBSECTION D Data Protection – Merchant Rules: Europe Region Only<br>D.1 Definitions<br>D.2 Processing of Personal Data<br>D.3 Data Transfers<br>D.4 Data Disclosures<br>D.5 Security of the Processing; Confidentiality; and Personal Data Breach<br>D.6 Data Protection and Security Audit<br>D.7 Liability<br>D.8 Applicable Law and Jurisdiction |
| **SUBSECTION E – Country Variations** | |
| Renamed SUBSECTION D – Country Variations to SUBSECTION E – Country Variations and made the following changes.<br>Renamed D.1 Israel to E.1 Israel and revised the section.<br>Renamed D.2 Romania to E.1 Romania and revised the section.<br>Renamed D.1 Russia to E.1 IsraelRussia and revised the section. | SUBSECTION E – Country Variations<br>E.1 Israel<br>E.2 Romania<br>E.3 Russia |

# Contents

**Audience** ..... **2**

**Summary of Changes, 25 May 2018** ..... **3**

**Chapter 1: Overview and Definitions** ..... **10**
1.1 Overview ..... 10
1.2 Definitions ..... 10
1.3 Interpretation ..... 14

**Chapter 2: Customers and Customer Service Providers** ..... **15**
2.1 Customers ..... 15
2.2 Customer Service Providers ..... 15
2.3 Customer Technology Providers ..... 15
2.4 Wallet Registration ..... 16
2.5 Area of Use ..... 16
2.6 Reservation of Rights ..... 16
2.7 Ownership and Control of the Wallet ..... 17
2.8 Conflict with Law ..... 17
2.9 Compliance ..... 17
2.10 Licenses ..... 18
2.10.1 License of Masterpass Property ..... 18
2.10.2 Licenses of Customer Trademarks ..... 18
2.11 Obligations of a Sponsor ..... 18
2.12 Name Change ..... 18
2.13 Fees, Assessments and Other Payment Obligations ..... 19
2.14 Trademarks and Service Marks ..... 19
2.14.1 Right to Use the Marks ..... 19
2.14.2 Misuse of a Mark ..... 20
2.14.3 Required Use ..... 20
2.14.4 Review of Solicitations ..... 20
2.15 Participation and License Not Transferable ..... 20
2.16 Sanctions Compliance Program ..... 20
2.17 Product Requirements ..... 21
2.17.1 Functionality Requirements ..... 21
2.17.1.1 Compliance with Specifications ..... 21
2.17.1.2 Tokenization, Digitization and Credential Management ..... 21
2.17.1.3 Device Scanning and Wallet Selector ..... 21
2.17.1.4 Transaction History Feature ..... 21

2.17.1.5 Customer Support ..... 21
2.17.1.6 No Interference ..... 21
2.17.2 Security Requirements ..... 22
2.17.3 Testing Requirements ..... 22
2.17.4 Additional Requirements ..... 22
2.18 Privacy and Data Protection ..... 23
2.18.1 Compliance ..... 23
2.18.2 Safeguards ..... 23
2.18.3 Security Incidents ..... 23
2.18.4 Governmental Request for Personal Data ..... 24
2.18.5 Malware Prevention ..... 24
2.18.6 Subcontractors ..... 24
2.18.7 Data Transfers ..... 25
2.19 Mastercard's Use of Personal Data ..... 25
2.20 Examination and Audit ..... 26
2.21 Provision and Use of Information ..... 26
2.21.1 Obligation to Provide Information ..... 26
2.21.2 Use of Mastercard Information ..... 27
2.21.3 Limitation on the use of Reporting ..... 27
2.21.4 Confidential Information ..... 27
2.22 Safeguard Card Account and Transaction Information ..... 27
2.23 Integrity of Brand and Network ..... 27
2.24 Export ..... 28
2.25 Indemnification ..... 28
2.26 Disclaimer ..... 29
2.27 Limitation of Liability ..... 29
2.28 Termination ..... 30
2.28.1 Termination by Mastercard ..... 30
2.28.2 Voluntary Termination ..... 32
2.28.3 Suspension and Amendment of Participation in Lieu of Termination ..... 32
2.28.4 Survival ..... 32
2.28.5 Effect of Termination; Wind-Down Period ..... 32
2.29 No Waiver ..... 32
2.30 Choice of Laws ..... 33

**Chapter 3: Merchants and Merchant Service Providers ..... 34**
3.1 Merchants ..... 34
3.2 Merchant Service Providers ..... 34
3.3 Merchant Technology Providers ..... 34
3.4 Merchant Rules ..... 35
3.5 Merchant Obligations ..... 35
3.6 Use of the Marks ..... 36

3.7 Conflict with Law....36
3.8 Compliance....36
3.9 Examination and Audit....36
3.10 Grant of License....37
3.11 Merchant Must Display the Masterpass Acceptance Brand....37
3.12 Merchant Advertising....38
3.13 Merchant Marks, Product Descriptions and Images....38
3.14 Wallet Acceptance Requirements....38
3.14.1 Non-Discrimination....38
3.14.2 Specifications....38
3.14.3 Updates....39
3.14.4 Outages....39
3.14.5 CVV Data....39
3.14.6 Implementing Checkout Postback....40
3.14.7 Merchant Customer Service....40
3.15 Masterpass Prohibited Practices....40
3.15.1 Merchant Acceptable Use Requirements....40
3.15.2 Minimum/Maximum Transaction Amount Prohibited....41
3.15.3 Transaction Processing without Confirmation Prohibited....41
3.16 Merchant Not to Charge Fees....41
3.17 Existing Network Requirements....41
3.18 PCI Compliance....41
3.19 Merchant Service Provider Agreement with Merchants....42
3.20 Merchant Service Provider Obligations....42
3.21 Privacy and Data Protection; Data Usage....43
3.21.1 Compliance....43
3.21.2 Safeguards....43
3.21.3 Security Incidents....43
3.21.4 Governmental Request for Personal Data....44
3.21.5 Malware Prevention....44
3.21.6 Subcontractors....44
3.21.7 Data Transfers....44
3.21.8 Merchant Use....44
3.21.9 Merchant Service Provider Use....45
3.21.10 Device Scanning and Wallet Selector....46
3.21.11 Use by Mastercard....46
3.22 Provision and Use of Information....47
3.22.1 Obligation to Provide Information....47
3.22.2 Use of Mastercard Information....47
3.22.3 Limitation on the use of Reporting....47
3.22.4 Confidential Information....47
3.23 Safeguard Card Account and Transaction Information....48
3.24 Integrity of Brand and Network....48

3.25 Export....48
3.26 Indemnification....48
3.27 Disclaimer....49
3.28 Limitation of Liability....49
3.29 Termination....50
3.29.1 Voluntary Termination....50
3.29.2 Suspension or Termination by Mastercard....50
3.29.3 Effect of Termination....50
3.30 Choice of Laws....51

**Chapter 4: Europe Region Variations....52**
Organization of this Chapter....52
SUBSECTION A....52
A.1 Choice of Laws....52
A.2 Use of Mastercard Information....52
A.3 Suspension or Termination by Mastercard....53
SUBSECTION B Data Protection – Mastercard-Hosted Wallet: Europe Region only....53
B.1 Definitions....53
B.2 Processing of Personal Data....54
B.3 Data Transfers....55
B.4 Data Disclosures....55
B.5 Security of the Processing; Confidentiality; and Personal Data Breach....55
B.6 Data Protection and Security Audit....56
B.7 Liability....56
B.8 Applicable Law and Jurisdiction....57
B.9 Public Authority's or Regulator's Requests....57
SUBSECTION C Data Protection – Partner-Hosted Wallet: Europe Region only....57
C.1 Definitions....57
C.2 Roles of the Parties....58
C.3 Obligations of Customer....58
C.4 Obligations of Mastercard....59
C.5 Data Transfers....60
C.6 Sub-Processing....60
C.7 Security of the Processing; Confidentiality; and Personal Data Breach....61
C.8 Data Protection Audit....61
C.9 Liability Towards Data Subjects....62
C.10 Applicable Law and Jurisdiction....62
SUBSECTION D Data Protection – Merchant Rules: Europe Region Only....62
D.1 Definitions....62
D.2 Processing of Personal Data....63
D.3 Data Transfers....64
D.4 Data Disclosures....64

D.5 Security of the Processing; Confidentiality; and Personal Data Breach..... 64
D.6 Data Protection and Security Audit..... 65
D.7 Liability..... 65
D.8 Applicable Law and Jurisdiction..... 66
SUBSECTION E – Country Variations..... 66
E.1 Israel..... 66
E.2 Romania..... 66
E.3 Russia..... 67

**Chapter 5: United States Region Variations..... 68**
Organization of this Chapter..... 68
3.14.8 Routing Choices..... 68

**Notices..... 69**

# Chapter 1 Overview and Definitions

## 1.1 Overview

Customers, Customer Service Providers, Merchants and Merchant Service Providers participating in the Masterpass Program agree to comply with the applicable Standards, including these *Masterpass Operating Rules*, as they may be amended from time to time. These *Masterpass Operating Rules* apply to all Wallet and Merchant implementations, and govern the conduct of Customers, Customer Service Providers, Merchants and Merchant Service Providers, and activities related to their participation in the Program. Mastercard has the right in its sole discretion to interpret, amend, and enforce the Standards. Mastercard reserves the right to limit, suspend or terminate a Customer's, Customer Service Provider's, Merchant's or Merchant Service Provider's participation in the Program.

## 1.2 Definitions

The following terms shall have the meanings ascribed below. Any capitalized term not defined herein may be found in the Definitions portion of the *Mastercard Rules* as that document may be amended from time to time. In the event of a conflict between the definition of a term set forth herein and the definition of a term set forth in the *Mastercard Rules*, the definition set forth herein shall apply.

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

**"API Specifications"** means the *Masterpass Partner-Hosted Wallet Integration Guide*, the *Merchant Integration Guide* and any other technical and operational specifications provided or made available by Mastercard from time to time with respect to a Customer's participation in the Program.

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

**"Customer"** means a Customer as defined in the *Mastercard Rules* that provides a user access to a Wallet either directly or through a Customer Service Provider.

**"Customer Service Provider"** means a Service Provider (as defined in *Mastercard Rules*) that provides certain Masterpass Program-related services to a Customer.

**"Customer Service Provider Account"** means an account established via the DevZone portal (or any other portal designated by Mastercard from time to time) to allow a Customer Service Provider to access the resources needed to provide Program-related services to a Customer.

**"Customer Technology Provider"** means a Technology Provider providing Program-related services to a Customer.

**"CVV Data"** means the three or four digit card security code 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 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.

**"Digital Wallet"** means functionality (a) by which account data provided by a user is stored electronically for the purpose of effecting a payment transaction initiated by the user at a Merchant and transmitted to the Merchant, or to its Acquirer, or the Acquirer's service provider to facilitate such payment transaction and (b) that may include value-added services.

**"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 written 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 the Corporation as defined in the *Mastercard Rules*.

**"Mastercard-Hosted Wallet"** means a Wallet hosted and operated by Mastercard.

**"Masterpass API"** means Mastercard's application programming interface between a Customer's Partner-Hosted Wallet and the Masterpass Network.

**"Masterpass Acceptance Brand"** means technology enabled on, and branding incorporated into, a Merchant's web site or other e-commerce application through which users can initiate payment transactions using their Wallet. The Masterpass Acceptance Brand includes the *Masterpass Button* and the *Masterpass Mark* (as required by Mastercard from time to time and described in the Masterpass Materials), which indicates a Merchant's participation in the Masterpass Network.

**"Masterpass Marks"** means the names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks associated with the Masterpass Acceptance Brand and the Masterpass Program from time to time in Mastercard's sole and absolute discretion and made available for use by Customers, Customer Service Providers, Merchants and Merchant Service Providers and other authorized entities.

**"Masterpass Materials"** means all materials made available by Mastercard to a Customer, Customer Service Provider, Merchant or Merchant Service Provider from time to time that are relevant to that entity's participation in the Program. These materials include, without

limitation, these *Masterpass Operating Rules*, the Masterpass Program Guides, the Masterpass API, the Masterpass Marks, the Masterpass Acceptance Brand, and the Specifications.

**"Masterpass 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.

**"Masterpass Network"** means a globally integrated network of Merchants that participate in the Masterpass Program.

**"Masterpass Program"** or **"Program"** means services offered by Mastercard, including the transmission of payment information, shipping information or any other Personal Data between a Wallet and a Merchant, to both enable payment using credentials stored in, and provide enhanced value-added services in connection with, Wallets. The Masterpass Program includes the Masterpass Network, Masterpass Acceptance Brand, and Wallets.

**"Masterpass Program Guides"** means the Masterpass guides and any other technical and operational specifications provided or made available by Mastercard from time to time with respect to a Customer's, Customer Service Provider's, Merchant's or Merchant Service Provider's participation in the Program including integration and implementation guides, which are hereby incorporated by reference.

**"Merchant"** means, for the purpose of these *Masterpass Operating Rules*, a Merchant (as defined in the Standards), including a Merchant that accepts payment cards from other payment networks, that is participating in the Masterpass Program.

**"Merchant Account"** means an account established via the Masterpass Merchant Portal to allow a Merchant to access the resources needed to display the Masterpass Acceptance Brand.

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

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

**"Merchant Service Provider"** means a Service Provider providing Program-related services to a Merchant.

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

**"Merchant Specifications"** means the *Masterpass Merchant Integration Guide* and any other technical and operational specifications provided or made available by Mastercard from time to time with respect to a Merchant's participation in the Program.

**"Merchant Technology Provider"** means a Technology Provider providing Program-related services to a Merchant.

**"Partner-Hosted Wallet"** means a Wallet hosted and operated by a Customer, or on behalf of a Customer by a Customer Service Provider, and that is compliant with the API

Specifications. A Wallet hosted but not operated by Mastercard shall be considered a "Partner-Hosted Wallet" hereunder.

**"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 Data Protection Directive 95/46/EC and e-Privacy Directive 2002/58/EC as amended by Directive 2009/136/EC and any relevant national implementing legislation, as well as guidance and recommendations from the competent Regulators; (b) the Gramm-Leach-Bliley Act; (c) applicable laws regulating unsolicited email communications; (d) applicable laws relating to security breach notifications; (e) applicable laws imposing minimum security requirements; (f) applicable laws requiring the secure disposal of records containing certain Personal Data; (g) applicable laws regulating banking secrecy and outsourcing requirements; (h) applicable laws regulating international data transfers and/or on-soil requirements; (i) applicable laws regulating incident reporting and data breach notification requirements, including guidelines and recommendations from the competent Regulators; (j) other similar applicable laws; (k) to the extent applicable, the Payment Card Industry Data Security Standards (PCI DSS), and (*l*) 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 Customer, Customer Service Provider, a Merchant or a Merchant Service Provider is required to provide to Mastercard, whether on a one-time or repeated basis, pertaining to its participation in the Masterpass Program.

**"Service Provider"** means a Service Provider as defined in the *Mastercard Rules* providing Program-related services.

**"Service Provider Specifications"** means the *Masterpass Service Provider Integration Guide* and any other technical and operational specifications provided or made available by Mastercard from time to time with respect to a Service Provider's participation in the Program.

**"Specifications"** means the API Specifications, Merchant Specifications and the Service Provider Specifications.

**"Standards"** means the *Mastercard Rules*, these *Masterpass Operating Rules*, the *Masterpass Branding Requirements* (or any equivalent documentation made available by Mastercard from

time to time) and all Masterpass Materials, in each case as in effect and amended from time to time.

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

**"Wallet"** means a Digital Wallet that has been approved by Mastercard to participate in the Masterpass Program either as a Partner-Hosted Wallet or a Mastercard-Hosted Wallet.

## 1.3 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 *Masterpass Operating Rules* and not to any particular chapter, subsection or clause hereof; and (h) the headings, captions, headers, footers and version numbers contained in these *Masterpass Operating Rules* are inserted for convenience only and shall not affect the meaning or interpretation of these *Masterpass Operating Rules*.

# Chapter 2 Customers and Customer Service Providers

## 2.1 Customers

A Customer may distribute its Wallet and/or may sponsor a Customer Service Provider serving as an Independent Sales Organization (ISO) as defined under the *Mastercard Rules* to distribute a Wallet. A Customer is responsible for and must itself manage, direct, and control all services performed by itself, and its Customer Service Providers and Customer Technology Providers. A Customer is responsible for its Wallet, and its actions (or inactions) and the actions (or inactions) of its Customer Service Providers and Customer Technology Providers or any other third party it uses in connection with its participation in the Program. The Customer must exercise a good faith commercial effort to implement and use best practices in performing Program-related services.

## 2.2 Customer Service Providers

A Customer Service Provider may participate in the Program and perform Program-related services for Customers in connection with a Wallet only if (i) said Customer Service Provider is registered with Mastercard as a Customer Service Provider in accordance with the *Mastercard Rules* and (ii) said Customer Service Provider has been registered with Mastercard by the Customer for such Program-related services.

The entity must maintain its registration as a Customer Service Provider in good standing with Mastercard while it is providing Program-related services. Additionally, any entity performing Program-related services must create a Customer Service Provider account and must continue to update registration and account information promptly.

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

## 2.3 Customer Technology Providers

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

required by Mastercard regarding such Customer Technology Provider and/or the services it provides.

## 2.4 Wallet Registration

A Customer may only participate in the Program with the express prior consent of Mastercard. A Customer must use the Masterpass Network, which is deemed to be proprietary to Mastercard, for the sole purpose of providing Program-related services and must not use or permit use for any other purpose without the prior express written consent of Mastercard.

Prior to connecting to the Masterpass Network, and as a condition of Program participation, the Customer must register its Wallet via the Masterpass registration process, which includes passing the Wallet certification process. The Customer must submit all information and material required by Mastercard (including but not limited to the Masterpass Registration Form) in connection with the Partner-Hosted Wallet registration to wallet_partners@mastercard.com at least 90 days prior to a planned launch as a Wallet. Customers must demonstrate compliance with any certification processes required by Mastercard, including the Wallet certification process, prior to distributing a Wallet. Wallets may not be distributed to users or otherwise and/or bear the Masterpass Mark prior to approval of compliance by Mastercard.

Mastercard will determine the requirements for providing a Mastercard-Hosted Wallet on behalf of Customer, which includes registration via the Wallet registration process.

## 2.5 Area of Use

Each Customer may distribute or operate a Wallet solely in the Area of Use in which the Customer has been granted a License. If the License does not specify an Area of Use, the License is deemed to authorize the Customer to use the Mark only in the country or countries Mastercard determines to be the Customer's Area of Use.

## 2.6 Reservation of Rights

Mastercard reserves the right:

1. To approve, reject, or terminate any Customer's, Customer Service Provider's or other entity's participation in the Program, or any Wallet associated therewith;
2. To require that any previously approved Wallet be modified;
3. To withdraw its approval of any Wallet and require its termination from the Masterpass Program; and
4. To terminate any Customer's, Customer Service Provider's or other entity's participation in the Program in accordance with these *Masterpass Operating Rules*.

A Customer may request that Mastercard's Chief Innovation Officer review the rejection or withdrawal of the approval of a Customer's participation in the Program by written request to Mastercard within 30 days of receipt of the notice of rejection or withdrawal of approval. Any decision by Mastercard's Chief Innovation Officer is final and not appealable.

## 2.7 Ownership and Control of the Wallet

A Wallet must be, and shall be deemed to be, Owned and Controlled by a Customer at all times even when the Wallet is distributed or managed by a Customer Service Provider.

## 2.8 Conflict with Law

A Customer, Customer Technology Provider or a Customer Service Provider is not required to undertake any act as part of its participation in the Program that is unambiguously prohibited by applicable law or regulation.

## 2.9 Compliance

Each Customer, Customer Technology Provider and Customer Service Provider must conduct activities related to their participation in the Program in full compliance with all applicable laws and regulations.

Each Customer, Customer Technology Provider and Customer Service Provider must conduct all activity and otherwise operate in a manner that is financially sound and so as to avoid risk to Mastercard and to other participants in the Program.

Each Customer must, and must ensure that its Customer Service Providers and Customer Technology Providers, fully cooperate with any effort by Mastercard and Mastercard's representatives to evaluate the Customer's or its Wallet's compliance with the Standards, including these *Masterpass Operating Rules*. In the event that Mastercard determines that a Customer, a Customer Service Provider or a Customer Technology Provider is not complying or may not on an ongoing basis comply with the aforementioned requirements, Mastercard may require a Customer, a Customer Service Provider or a Customer Technology Provider to take action, and Mastercard itself may take action, as Mastercard deems necessary or appropriate to address noncompliance with the *Masterpass Operating Rules* and to otherwise safeguard the integrity of the Masterpass Program.

## 2.10 Licenses

### 2.10.1 License of Masterpass Property

Effective upon approval of the Masterpass Registration Form by Mastercard, Mastercard grants to the Customer and its Customer Service Provider(s) a non-exclusive, non-transferable license to: (i) use, access and connect to the Masterpass API to connect a Customer's Partner-Hosted Wallet to the Masterpass Network; (ii) use, access, connect to, publicly perform and display any other portion of the Masterpass intellectual property, as applicable, for the purposes of operating a Partner-Hosted Wallet; and (iii) use the Masterpass Marks in accordance with Section 2.14 (*Trademarks and Service Marks*) below and the current brand requirements as set forth in the *Masterpass Branding Requirements* (or any equivalent documentation made available by Mastercard from time to time), which are incorporated into these *Masterpass Operating Rules* by reference. This license shall remain in effect solely until, and shall automatically terminate simultaneously when, the Customer's and/or its Customer Service Provider(s)' participation in the Program is terminated in accordance with the Standards and these *Masterpass Operating Rules*.

### 2.10.2 Licenses of Customer Trademarks

Effective upon approval of the Masterpass Registration Form by Mastercard, Customer grants to Mastercard and its Affiliates a worldwide, non-exclusive, non-transferable, royalty-free license to use, reproduce, publicly perform and display Customer's and/or its Customer Service Provider(s)' trademarks and copyrights (including, the Customer's card art), as applicable, in connection with their participation in the Masterpass Program.

## 2.11 Obligations of a Sponsor

Each Principal and Association Customer that sponsors one or more Affiliate Customers as a Customer or Customers under these *Masterpass Operating Rules* must cause each such Affiliate Customer to comply with the Standards applicable to that Affiliate Customer's participation in the Program. The Principal and Association Customer is liable to Mastercard and to all other Customers for Program-related activity of any Affiliate Customer sponsored by the Principal and Association Customer and for any failure by such sponsored Affiliate Customer to comply with a Standard or with applicable law or regulation.

Each Principal or Association Customer must advise Mastercard promptly if an Affiliate Customer offering a Wallet ceases to be sponsored by the Principal or Association Customer or changes its name or has a transfer of Ownership or Control.

## 2.12 Name Change

A Customer must provide written notice received by Mastercard at least thirty (30) calendar days before the effective date of any proposed Customer or Wallet name change. A Customer

that proposes to change its name must promptly undertake necessary or appropriate action to ensure that its participation in the Program discloses the true identity of the Customer.

## 2.13 Fees, Assessments and Other Payment Obligations

Each Customer, both for itself and on behalf of its Customer Service Providers, is responsible to timely pay to Mastercard all fees, charges, assessments and the like applicable to their participation in the Program as may be in effect from time to time.

## 2.14 Trademarks and Service Marks

### 2.14.1 Right to Use the Marks

Customers participating in the Program have the right to use one or more of the Masterpass Mark(s) pursuant to Section 2.10.1 (*License of Masterpass Property*) above.

No additional interest in the Masterpass Mark(s) is granted with the grant of a right to use the Masterpass Mark(s). A Customer is responsible for all costs and liabilities resulting from or related to its use of a Masterpass Mark(s). The right to use the Masterpass Mark(s) is non-exclusive and non-transferable.

The right to use the Masterpass Mark(s) cannot be sublicensed or assigned, whether by sale, consolidation, merger, amalgamation, operation of law, or otherwise, without the express written consent of Mastercard.

Mastercard makes no express or implied representations or warranties in connection with the Masterpass Mark(s) and Mastercard specifically disclaims all such representations and warranties. Any use of the Masterpass Marks (or any other mark representing Mastercard's digital acceptance) in connection with the Customer's Wallet (whether by Customer, its Customer Service Provider, or otherwise), including any associated goodwill, will inure to Mastercard's benefit.

### 2.14.2 Misuse of a Mark

Each Customer must promptly notify Mastercard whenever it learns of any misuse of any Masterpass Mark or of any attempt to copy or infringe on any of the Masterpass Mark(s).

### 2.14.3 Required Use

Masterpass Mark(s) must be used in accordance with the current brand requirements as set forth in the *Masterpass Branding Requirements*, which are incorporated into these *Masterpass Operating Rules* by reference.

### 2.14.4 Review of Solicitations

Mastercard reserves the right to review samples of those materials and to approve or refuse to approve use of a Solicitation. Amended samples, if required as a result of this review, also must be forwarded to Mastercard for review.

## 2.15 Participation and License Not Transferable

A Customer and its Customer Service Provider(s) may not transfer or assign any rights or responsibilities it may have in connection with its participation in the Program or any license to use the Masterpass Marks whether by sale, consolidation, merger, operation of law, or otherwise, without the express written consent of Mastercard.

## 2.16 Sanctions Compliance Program

A Customer must have implemented a sanctions compliance program that, at a minimum, contains the following elements:

Each Customer Service Provider, and each user for which the Customer has access to name information, is checked against the Specially Designated Nationals and Blocked Persons List (the **"SDN List"**) issued by the U.S. Treasury Department's Office of Foreign Assets Control (**"OFAC"**), at the time the relationship is established and on an ongoing basis; any Wallet activity with a Customer Service Provider or user that is found to be on the SDN List is immediately terminated.

No Wallet activity is conducted in a country subject to OFAC sanctions programs that impact payment services, or with the government of such a country. The list of countries subject to OFAC sanctions programs may change from time to time. More information on U.S. sanctions is available at http://www.treasury.gov/resource-center/sanctions.

Any questions regarding sanctions compliance can be directed to trade_sanctions@mastercard.com.

# 2.17 Product Requirements

## 2.17.1 Functionality Requirements

### 2.17.1.1 Compliance with Specifications

A Partner-Hosted Wallet must comply with all required elements of the then-current version of the Masterpass Materials (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 Customer 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. A Customer 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 API Specifications. Recertification will be required at Mastercard 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.

### 2.17.1.2 Tokenization, Digitization and Credential Management

In order to support the tokenization, digitization and credential management of cards provisioned into a Wallet, the Customer and/or the Customer Service Provider, as applicable, must comply with the registration process, technical specifications and Standards set out by Mastercard and/or the payment network under which mark(s) the cards are issued, as applicable.

### 2.17.1.3 Device Scanning and Wallet Selector

Each Wallet shall implement the Masterpass Materials and technology required for device scanning and display of the wallet selector view, where available in the Customer's Area of Use and supported by the operating system of the user's device.

### 2.17.1.4 Transaction History Feature

With respect to payment cards not issued by the Customer, the Wallet may only display transaction history for each card provisioned into the Wallet in accordance with the technical specifications made available by Mastercard and/or the payment network under which mark(s) the cards are issued, as applicable from time to time.

### 2.17.1.5 Customer Support

The Customer must establish customer support policies and procedures in line with industry best practices.

### 2.17.1.6 No Interference

The Customer must not engage in forced steering away from a user's chosen payment option after a user has initiated a purchase transaction via a Wallet. The Customer must prohibit the advertisement of competitive checkout solutions when a user is conducting a transaction via a Wallet (noncompetitive marketing is permitted). In the event the issuer wallet participates in

more than one network's offerings, the customer may not be "force steered" to any alternate payment option after choosing to "Buy with Masterpass".

### 2.17.2 Security Requirements

A Partner-Hosted Wallet must at all times be compliant with the Payment Card Industry Data Security Rules (PCI DSS) and the Payment Application Data Security Rules (PA DSS), and any local regulations as applicable. The Customer agrees to promptly provide Mastercard with documentation evidencing compliance of its Partner-Hosted Wallet or Customer-hosted features of the Wallet (including, partner log-in and direct provisioning as described in the API Specifications) with PCI DSS and/or PA DSS when requested by Mastercard. This compliance must be determined by a Qualified Security Assessor (QSA) when applicable. Customers will ensure only PCI compliant service providers are used in connection with their Wallet.

In addition, the Customer must:

1. Establish a multi-factor system for user login/wallet access. (for example; user name and password is one layer; one time password or device cookie is a second layer);
2. Provide, upon request, a summary of vulnerability assessment, including the date and scope of the testing, and the process invoked (Mastercard shall not request such information more than once a year unless the Wallet experiences a data breach or Mastercard reasonably believes that the Wallet's security may be compromised);
3. Ensure continued compliance with PCI standards including yearly recertification of the Partner-Hosted Wallet;
4. Ensure security treatment for all account data stored in the Partner-Hosted Wallet is equal if not exactly the same, regardless of the Customer or other issuer that issued the user's payment cards; and
5. Establish methods for the secure handling of production and sandbox keys.

Mastercard, via the Masterpass System, will provide program level security functions and services that a Customer will be required to accommodate in its Partner-Hosted Wallet.

### 2.17.3 Testing Requirements

Customers must perform testing as mandated by Mastercard. This testing must demonstrate that a Partner-Hosted Wallet is able to successfully complete transactions prior to any launch. The Partner-Hosted Wallet must also be successfully tested after each new version of the code is released. Advance notice regarding testing will be provided to Customers. All testing as mandated by Mastercard in these *Masterpass Operating Rules* is at the Customer's expense.

### 2.17.4 Additional Requirements

In addition to the aforementioned requirements, a Customer must, itself or through its Customer Service Provider:

1. Maintain the minimum service levels determined by Mastercard from time to time including Partner-Hosted Wallet response time and overall availability, and Wallet customer support availability;
2. Complete any necessary security due diligence review as may be required by Mastercard;
3. Complete the Masterpass Registration Form and obtain a Wallet Identifier;

4. Each time a system release introduces a material change to how Personal Data is processed through a Wallet, Mastercard will provide a Customer with notice of such material change. The Customer is responsible for ensuring that such processing of Personal Data is done in compliance with all applicable laws and regulations, including ensuring that all users are properly informed, and if necessary, have given proper consent, and, to the extent applicable, filing any necessary documents with the local regulatory authority, in each case, prior to updating its systems with the relevant system release;
5. Comply with the user experience requirements and/or guidelines made available by Mastercard from time to time; and
6. Provide information on the performance of the Wallet to Mastercard at the frequency and in the format required by Mastercard including (i) monthly report of number of new users and number of transactions and (ii) any information required to be reported through the Masterpass reporting APIs, when available.

## 2.18 Privacy and Data Protection

### 2.18.1 Compliance

Each Customer shall, and shall ensure that all of their Customer Service Providers, comply with Privacy and Data Protection Requirements in connection with their participation in the Program. Each Customer shall be responsible for filing notifications to and/or obtaining approvals from competent regulators as legally required under applicable Privacy and Data Protection Requirements.

To the extent a Customer processes Personal Data of a resident of the European Economic Area or otherwise subject to EU Data Protection Law, the Customer must also comply with Sub-Section B or C applicable to the Europe Region.

### 2.18.2 Safeguards

Each Customer shall, and shall ensure that all of their Customer 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 Customer's Wallet, a **"Customer Security Incident"** and with respect to Personal Data Mastercard processes through such Customer's Wallet, a **"Mastercard Customer Security Incident"**), (d) ensure the proper disposal of Personal Data, and (e) regularly test or otherwise monitor the effectiveness of the safeguards.

### 2.18.3 Security Incidents

(a) Except to the extent prohibited by applicable law, each of the Customers and Mastercard shall inform the other in writing, in accordance with the account data compromise event procedures set forth in the *Standards*, in a commercially reasonable timeframe upon discovery

of any Customer Security Incident, with respect to Customer, and a Mastercard Customer Security Incident, with respect to Mastercard, 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 Masterpass Express program that may result in such incidents.

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

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

### 2.18.4 Governmental Request for Personal Data

Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, each of Mastercard and each Customer 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 Program that relates to a Customer's Wallet. 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.

### 2.18.5 Malware Prevention

Mastercard and each Customer will take commercially reasonable diligent measures to ensure that Malware is not coded or introduced into its respective systems interacting with the Program or Mastercard's or a Customer's systems interacting therewith. Mastercard and each Customer 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 Program or Mastercard's or Customer's systems interacting therewith, Mastercard and the affected Customer(s) will cooperate and use commercially reasonable efforts to promptly communicate, and diligently work to remedy the effects of, the Malware.

### 2.18.6 Subcontractors

Mastercard and each Customer shall remain liable towards the others for the Processing of Personal Data carried out by its respective subcontractors in connection with the Program and shall bear responsibility for the correct fulfillment of their respective obligations. Mastercard and each Customer 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 2.18 and shall prohibit its subcontractors to Process Personal Data other than as instructed.

### 2.18.7 Data Transfers

Personal Data Processed in connection with the Program 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 either (a) an intragroup agreement executed by and among Mastercard and Mastercard Affiliates, which agreement is in accordance with the Standard Contractual Clauses issued by the European Commission Directorate-General Justice pursuant to Commission Decisions C(2010)593, C(2004)5721 and 2001/497/EC or (b) Mastercard's Binding Corporate Rules, as defined in sections B3 and C5 of these *Masterpass Operating Rules*.

## 2.19 Mastercard's Use of Personal Data

A Customer must provide notice and obtain consent from all users necessary to ensure that, at a minimum, Mastercard has the right to use Personal Data collected, stored or processed in connection with a Wallet for the following purposes:

1. Create and manage an online account, provide Program related products and services, respond to user inquiries and provide customer service to respond to inquiries made by users;
2. Validate payment card information, authenticate a user's identity and tokenize a user's payment credentials;
3. Mobile application device scanning to identify each Wallet on a consumer's mobile device and present information from each Wallet, including payment cards registered in such wallet and shipping address, in the Mobile Checkout View, as more fully described in Section 2.17.1.3.
4. Protect against and prevent fraud, unauthorized transactions, claims and other liabilities, and manage risk exposure and franchise quality;
5. Operate, evaluate, audit and improve the Program (including by developing new product features and services; managing communications; determining the effectiveness of advertising; analyzing Program related products, services and websites; facilitating the functionality of our websites; and performing accounting, auditing, billing, reconciliation and collection activities);
6. Assist third parties, including a Merchant or a Customer Service Provider, in the provision of products or services that are requested by a user;
7. 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;
8. For preparing and furnishing compilations, analyses and other reports of aggregated information in connection with the Program;
9. Enforce these *Masterpass Operating Rules*;
10. Comply with applicable legal requirements and industry standards and Mastercard policies;

11. Perform auditing, research and analysis in order to maintain, protect and improve our services; and
12. For any additional use of Personal Data necessary to implement a Program feature incorporated by Customer into its Wallet; and for other purposes for which the Data Subject to whom the Personal Data relates has provided explicit consent.

Mastercard may determine in its sole discretion the contents of the privacy notice and terms and conditions to be provided to users in order to obtain the consents required to operate a Mastercard-Hosted Wallet.

In the event that Mastercard provides Personal Data to a Customer or Customer Service Provider relating to their Mastercard-Hosted Wallet, the Customer shall only use such Personal Data for the purposes permitted by such privacy notice and otherwise in compliance with all applicable law and regulations.

## 2.20 Examination and Audit

Mastercard reserves the right to conduct an audit or examination of any Customer or Customer Service Provider to ensure full compliance with the Standards. Any such audit or examination is at the expense of the Customer or Customer 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 Customer Service Provider be unable or unwilling to cover the cost of such audit or examination, the audit or examination shall be at the responsible Customer's expense. Mastercard shall not exercise this right more than once a year unless Mastercard has reason to believe that the Customer or Customer Service Provider does not materially comply with the Standards.

## 2.21 Provision and Use of Information

### 2.21.1 Obligation to Provide Information

Upon request by Mastercard, and subject to applicable law and regulation, a Customer or Customer Service Provider must provide Reports to Mastercard, or to Mastercard's designee. Compliance with the foregoing obligation does not require a Customer or Customer Service Provider to furnish any information the disclosure of which, in the written opinion of the Customer's or Customer Service Provider's legal counsel, as applicable, is likely to create a significant potential legal risk to Customers or Customer Service Providers. To the extent that there is an obligation to provide a Report to Mastercard that the Customer or Customer Service Provider deems to disclose proprietary information of the Customer, such information will be treated by Mastercard with the degree of care deemed appropriate by Mastercard to maintain its confidentiality.

### 2.21.2 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 Customer or a Customer 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 Customer or a Customer Service Provider.

### 2.21.3 Limitation on the use of Reporting

Mastercard may use or disclose the Reports furnished by a Customer or Customer 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 its business (including by developing new products and services; managing our communications; determining the effectiveness of our advertising; analyzing our products, services and websites; facilitating the functionality of the Masterpass Program; 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 Masterpass Program.

### 2.21.4 Confidential Information

A Customer or a Customer Service Provider may receive information (whether written, oral, electronic, or otherwise) as part of participation in the Masterpass Program relating to Mastercard or to the Masterpass Program that is not freely available to the general public ("Confidential Information"). Each Customer and Customer 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 participation in the Masterpass Program; and (c) it will not otherwise disclose Confidential Information to any individual, company, or other third party.

## 2.22 Safeguard Card Account and Transaction Information

Each Customer, for itself and any third party, including its Customer Service Providers and each Customer Service Provider that may be afforded access to Transaction or Personal Data, or both, by or on behalf of the Customer, must safeguard and use or permit use of such information in accordance with the Standards. A Customer or a Customer 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.

## 2.23 Integrity of Brand and Network

In connection with the Program, a Customer or a Customer 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 Standards, damages or may damage the goodwill or reputation of Mastercard or of any Masterpass Mark, and the Customer or the Customer Service Provider will promptly cease engaging in or facilitating such action upon request of Mastercard.

In connection with the Program, a Customer or a Customer 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 Masterpass Network. Specific obligations will be defined in the Masterpass Materials.

## 2.24 Export

Customers and Customer Service Providers shall not import or export any of the Masterpass Materials without first obtaining Mastercard's written approval. If so permitted to import or export Masterpass Materials, then Customers and Customer Service Providers shall comply with all foreign and U.S. export and import regulations applicable with respect to the Masterpass Materials.

## 2.25 Indemnification

Each Customer and its Customer Service Providers and Customer Technology Providers (each, for the purposes of this Section 2.25, an **"Indemnifying Party"**) must protect, indemnify, and hold harmless Mastercard and Mastercard's parent and subsidiaries and affiliated entities, and each of the directors, officers, employees and agents of Mastercard and Mastercard's parent and subsidiaries and affiliated entities from any actual or threatened claim, demand, obligation, loss, cost, liability and/or expense (including, without limitation, actual attorneys' fees, costs of investigation, and disbursements) resulting from and/or arising in connection with any act or omission of the Indemnifying Party, its subsidiaries, or any person associated with the Indemnifying Party or its subsidiaries (including, without limitation, such Indemnifying Party's directors, officers, employees and agents, all direct and indirect parents, subsidiaries, and affiliates of the Indemnifying Party, the Indemnifying Party's customers in connection with its participation in the Program and/or other business, and the Indemnifying Party's suppliers, including, without limitation, Customer Service Providers and other persons acting for, on behalf of, or in connection with, the Indemnifying Party or a Merchant for which the Indemnifying Party acquires Transactions or transactions of another payment network, and/or any such Merchant's employees, representatives, agents, suppliers, or customers including any Data Storage Entity (**"DSE"**)), with respect to, or relating to:

1. Any activities of the Indemnifying Party related to its participation in the Program;
2. Any activities of any person, including a Customer Service Provider or Merchant associated with the Indemnifying Party and/or its subsidiaries related to their respective participation in the Program;
3. The compliance or non-compliance with the Standards by the Indemnifying Party;

4. The compliance or non-compliance with the Standards by any person, including a Customer Service Provider or Merchant associated with the Indemnifying Party and its subsidiaries;
5. Any other activity of the Indemnifying Party;
6. Direct or indirect access to and/or use of the Program or any Masterpass Materials (it being understood that Mastercard does not represent or warrant that the Program or any Masterpass Materials or any part thereof is or will be defect-free or error-free and that each Customer, Merchant or Customer Service Provider chooses to access and use or distribute, as the case may be, the Masterpass Network or access thereto at the Customer's, Merchant's or Customer Service Provider's sole risk and at no risk to Mastercard); or
7. Any other activity and any omission of the Indemnifying Party and any activity and any omission of any person associated with the Indemnifying Party, its subsidiaries, or both, including any activity that used and/or otherwise involved any of the Masterpass Materials or other assets.

## 2.26 Disclaimer

THE MASTERPASS PROGRAM AND MASTERPASS MATERIALS ARE PROVIDED ON AN "AS IS" BASIS WITHOUT ANY WARRANTY WHATSOEVER. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, MASTERCARD DOES NOT REPRESENT OR WARRANT THAT THE MASTERPASS PROGRAM OR ANY OTHER SYSTEM, PROCESS OR ACTIVITY ADMINISTERED, OPERATED, CONTROLLED OR PROVIDED BY OR ON BEHALF OF MASTERCARD (COLLECTIVELY, FOR PURPOSES OF THIS RULE, THE **"SYSTEMS"**) OR ANY OF THE MASTERPASS MATERIALS WILL MEET THE CUSTOMER'S OR SERVICE PROVIDER'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 AND, UNLESS OTHERWISE SPECIFICALLY STATED IN THE STANDARDS OR IN A WRITING EXECUTED BY AND BETWEEN MASTERCARD AND A CUSTOMER OR SERVICE PROVIDER, AS THE CASE MAY BE, THE SYSTEMS AND MASTERPASS MATERIALS ARE PROVIDED ON AN "AS-IS" BASIS AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY TYPE, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

## 2.27 Limitation of Liability

IN NO EVENT WILL MASTERCARD BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, ENHANCED OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, INDEMNIFICATION OR ANY OTHER COST OR EXPENSE INCURRED BY A CUSTOMER, A SERVICE PROVIDER OR ANY THIRD PARTY ARISING FROM OR RELATED TO USE OR RECEIPT OF THE SYSTEMS OR MASTERPASS MATERIALS, WHETHER IN AN ACTION IN CONTRACT OR IN TORT, AND EVEN IF THE CUSTOMER, THE SERVICE PROVIDER OR ANY THIRD PARTY HAS

BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EACH CUSTOMER AND SERVICE PROVIDER ASSUMES THE ENTIRE RISK OF USE OR RECEIPT OF THE SYSTEMS AND MASTERPASS MATERIALS.

ONLY IN THE EVENT THE LIMITATION OF LIABILITY SET FORTH IN THE IMMEDIATELY PRECEDING PARAGRAPH IS DEEMED BY A COURT OF COMPETENT JURISDICTION TO BE CONTRARY TO APPLICABLE LAW, SUBJECT TO THE PRECEDING SECTION, THE TOTAL LIABILITY, IN THE AGGREGATE, OF MASTERCARD TO A CUSTOMER, A SERVICE PROVIDER AND ANYONE CLAIMING BY OR THROUGH THE CUSTOMER OR SERVICE PROVIDER, FOR ANY AND ALL CLAIMS, LOSSES, COSTS OR DAMAGES, INCLUDING ATTORNEYS' FEES AND COSTS AND EXPERT-WITNESS FEES AND COSTS OF ANY NATURE WHATSOEVER OR CLAIMS EXPENSES RESULTING FROM OR IN ANY WAY RELATED TO THE SYSTEMS AND/OR MASTERPASS MATERIALS SHALL NOT EXCEED THE TOTAL COMPENSATION RECEIVED BY MASTERCARD FROM THE CUSTOMER OR SERVICE PROVIDER, RESPECTIVELY, FOR THE PARTICULAR USE OR RECEIPT OF OR ACCESS TO THE SYSTEMS OR MASTERPASS MATERIALS DURING THE TWELVE (12) MONTHS ENDING ON THE DATE THAT MASTERCARD WAS ADVISED BY THE CUSTOMER OR SERVICE PROVIDER OF THE SYSTEMS' OR MASTERPASS MATERIALS' CONCERN OR THE TOTAL AMOUNT OF USD 250,000 (FOR CUSTOMER) OR USD 25,000 (FOR SERVICE PROVIDER), WHICHEVER IS LESS. IT IS INTENDED THAT THIS LIMITATION APPLY TO ANY AND ALL LIABILITY OR CAUSE OF ACTION HOWEVER ALLEGED OR ARISING; TO THE FULLEST EXTENT PERMITTED BY LAW; UNLESS OTHERWISE PROHIBITED BY LAW; AND NOTWITHSTANDING ANY OTHER PROVISION OF THE STANDARDS.

## 2.28 Termination

A Customer's participation in the Program may terminate in one of two ways: termination by Mastercard or voluntary termination.

### 2.28.1 Termination by Mastercard

Mastercard, at its sole discretion, may terminate a Customer's participation in the Program effective immediately and without prior notice, if or in the event of:

1. Customer suspends payments within the meaning of Article IV of the Uniform Commercial Code in effect at the time in the State of Delaware, regardless of whether, in fact, the Customer is subject to the provisions thereof; or
2. Customer takes the required action by vote of its directors, stockholders, members, or other persons with the legal power to do so, or otherwise acts, to cease operations and to wind up the business of the Customer, such participation termination in Program-related activities to be effective upon the date of the vote or other action; or
3. Customer fails or refuses to make payments in the ordinary course of business or becomes insolvent, makes an assignment for the benefit of creditors, or seeks the protection, by the filing of a petition or otherwise, of any bankruptcy or similar statute governing creditors' rights generally; or

4. The government or the governmental regulatory authority having jurisdiction over the Customer serves a notice of intention to suspend or revoke, or suspends or revokes, the operations or the charter of the Customer; or
5. A liquidating agent, conservator, or receiver is appointed for the Customer, or the Customer is placed in liquidation by any appropriate governmental, regulatory, or judicial authority; or
6. Customer's failure to comply with Mastercard's AML Program or applicable law or regulation; or
7. Customer fails to engage in Program-related activity for thirty (30) consecutive days; or
8. Customer is no longer Licensed to use any of the Marks; or
9. Customer or Customer Service Provider fails to comply in all material respects with the Masterpass Materials; or
10. Customer (i) directly or indirectly engages in or facilitates any action or activity that is illegal, or that, in the good faith opinion of Mastercard, and whether or not addressed elsewhere in the Standards, has damaged or threatens to damage the goodwill or reputation of Mastercard or of any of its Marks; or (ii) makes or continues an association with a person or entity which association, in the good faith opinion of Mastercard, has damaged or threatens to damage the goodwill or reputation of Mastercard or of any of its Marks; or
11. Customer (i) provides to Mastercard inaccurate material information or fails to disclose responsive material information in or in connection with its Program-related registration or certification or (ii) at any other time, in connection with its Program-related participation fails to timely provide to Mastercard information requested by Mastercard and that the Customer is required to provide pursuant to its Program-related registration, certification or the Standards; or
12. Customer fails at any time to satisfy any of the applicable Participation eligibility criteria set forth in the Standards; or
13. Mastercard has reason to believe that the Customer is, or is a front for, or is assisting in the concealment of, a person or entity that engages in, attempts or threatens to engage in, or facilitates terrorist activity, narcotics trafficking, trafficking in persons, activities related to the proliferation of weapons of mass destruction, activity that violates or threatens to violate human rights or principles of national sovereignty, or money laundering to conceal any such activity. In this regard, and although not dispositive, Mastercard may consider the appearance of the Customer, its owner or a related person or entity on a United Nations or domestic or foreign governmental sanction list that identifies persons or entities believed to engage in such illicit activity; or
14. Within thirty (30) days of receipt of written notice by Mastercard requiring a Customer to confirm the accuracy of information provided by the Customer to Mastercard pursuant to its Program-related registration, certification or the Standards, the Customer does not demonstrate to the satisfaction of Mastercard that either: (i) the information provided was accurate; or (ii) with respect to any inaccurate information, such inaccurate information was provided to Mastercard through inadvertence or with a reasonable belief as to its truth and provide information sufficient to correct such inaccuracy.

### 2.28.2 Voluntary Termination

A Customer may voluntarily terminate Program-related participation by providing written notice and submitting documentation as then required by Mastercard. The notice must fix a date on which the termination will be effective, which must be at least thirty (30) days after date on which the notice is received by Mastercard.

### 2.28.3 Suspension and Amendment of Participation in Lieu of Termination

Mastercard may, in its sole discretion:

1. Suspend the participation of a Customer in the Masterpass Program; or
2. Amend the rights or obligations or both of a Customer with regard to the Program.

A Customer whose participation in the Program has been suspended must continue to comply with the Standards.

### 2.28.4 Survival

The termination, for any reason, of the Customer's participation in the Program will not affect: (a) the rights or obligations of the Customer or Mastercard against the other that have accrued on or prior to the termination; or (b) any rights or obligations that by their nature survive the termination.

### 2.28.5 Effect of Termination; Wind-Down Period

Unless otherwise directed by Mastercard, for ninety (90) days immediately following the effective date of termination, the Customer must reasonably cooperate with Mastercard to cease the display, distribution and any other use of marketing materials related to the Customer's participation in the Program, to ensure that users of the Wallet do not experience an abrupt cessation of service and otherwise to ensure an orderly winding up, continuation or transfer of the suspended or terminated Wallet.

Mastercard reserves the right to solicit users of a Wallet to transfer their account to a Masterpass by Mastercard wallet in the event a Customer's participation in the Masterpass Program is terminated.

## 2.29 No Waiver

A payment or credit by Mastercard to or for the benefit of a Customer that is not required to be made by the Standards will not be construed to be a waiver or modification of any Standard by Mastercard. A failure or delay by Mastercard to enforce any Standard or exercise any right of Mastercard set forth in the Standards will not be construed to be a waiver or modification of the Standard or of any of Mastercard's rights therein.

## 2.30 Choice of Laws

The substantive laws of the State of New York shall govern all disputes involving Mastercard, the Standards, and/or the Customer's or Customer Service Provider's participation in the Program without regard to conflicts. Any action initiated by a Customer or Customer Service Provider regarding and/or involving Mastercard, the Standards and/or any Customer or Customer 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 Customer or Customer 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 Customer and Customer Service Provider agrees that the Standards are construed under, and governed by, the substantive laws of the State of New York without regard to any choice or conflict of law provision or rule (whether of the State of New York or any other jurisdiction).

# Chapter 3 Merchants and Merchant Service Providers

## 3.1 Merchants

To participate in the Program and display the Masterpass Acceptance Brand, a Merchant must (a) accept Mastercard-branded payment cards, (b) be in good standing with its Acquirer, and (c) either (i) register by creating a Merchant Account, selecting the services it will receive, and agree to be bound by these *Masterpass Operating Rules*; or (ii) if accessing the Program via a Merchant Service Provider that is using the File or API based uploading feature, as defined in the Service Provider Specifications, agree to be bound by these *Masterpass Operating Rules*.

## 3.2 Merchant Service Providers

A Merchant Service Provider may participate in the Program and perform Program-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 Program-related services.

Each Merchant Service Provider must maintain their registration as a Merchant Service Provider in good standing with Mastercard while it is providing Program-related services. Additionally, any entity performing Program-related services must create a Merchant Service Provider account on the Masterpass 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.

Program-related services performed by any entity, which services directly or indirectly support or otherwise benefit a Merchant's participation in the Program 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 Standards, including without limitation these *Masterpass Operating Rules*.

## 3.3 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 Program-related services in connection with Merchant's participation in the Program 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.

## 3.4 Merchant Rules

Merchant, Merchant Service Provider(s) and Merchant Technology Provider(s) must agree to comply with the Standards, including these *Masterpass Operating Rules*, prior to displaying the Masterpass Acceptance Brand. Additional information can be found in the *Masterpass Merchant Implementation Guide*. Merchants are responsible for their Merchant Service Provider and Merchant Technology Providers' compliance with these *Masterpass Operating Rules* (and the Standards, where applicable).

## 3.5 Merchant Obligations

Each Merchant must:

1. Notify its Acquirer in writing of its use of any Merchant Service Provider(s) in connection with its participation in the Program;
2. Submit to its Acquirer any Wallet Identification Number ("WID"), as supplied by Mastercard;
3. Be eligible to register and participate in the Program and have the right, power, and ability to comply with these *Masterpass Operating Rules*;
4. Provide to Mastercard, either directly or through its Merchant Service Provider, the name or business name under which it sell goods and services;
5. 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;
6. 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 participation in the Program;
7. Provide all necessary notices to and obtain all necessary consents from users as required by law to transfer Personal Data to Mastercard for its use in connection with the Program pursuant to these *Masterpass Operating Rules*;
8. Not facilitate transactions that are prohibited by Mastercard's Acceptable Use Policy (see Section 3.15.1 for additional information);
9. Not use participation in the Program, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Services;
10. 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 Program;
11. Only use, and ensure that its Merchant Service Providers only use, Personal Data provided by Mastercard for purposes of participating in the Program as contemplated in these *Masterpass Operating Rules*;
12. Not, by performing its obligations hereunder, violate any other agreement to which it is a party; and

13. 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 Program.

## 3.6 Use of the Marks

Any use of the Masterpass 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 *Masterpass Branding Requirements*, which are incorporated into these *Masterpass Operating Rules* by reference.

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

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

## 3.7 Conflict with Law

A Merchant, Merchant Service Provider or Merchant Technology Provider is not required to undertake any act as part of its participation in the Program that is unambiguously prohibited by applicable law or regulation.

## 3.8 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 Standards, including these *Masterpass Operating Rules*. 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 the *Masterpass Operating Rules* and to otherwise safeguard the integrity of the Masterpass Program.

## 3.9 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 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 Standards.

## 3.10 Grant of License

During the term of the Merchant's participation in the Program, Mastercard grants (i) Merchant, and by its use of the Masterpass Acceptance Brand the Merchant accepts, and (ii) Merchant Service Providers a non-exclusive, non-transferable, non-sub licensable, royalty-free, revocable, worldwide license to use the Masterpass Acceptance Brand and Masterpass Marks (including "Masterpass," "Masterpass Online," "Buy with Masterpass," "Masterpass Wallet," "Masterpass Checkout Services," "Masterpass Acceptance Brand," "Masterpass Network," "Masterpass API," and other related designs, graphics, logos, page headers, button icons, scripts, and service names as may be designated by Mastercard from time to time), solely (a) to identify that Masterpass 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 *Masterpass Branding Requirements* (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 participation in the Masterpass Program is terminated in accordance with the Standards and these *Masterpass Operating Rules*. The Merchant and Merchant Service Provider shall promptly cease use of the Masterpass Marks and Masterpass Acceptance Brand if their participation in the Program has been suspended or terminated.

## 3.11 Merchant Must Display the Masterpass Acceptance Brand

A Merchant must prominently display the Masterpass Acceptance Brand in accordance with the Standards and Specifications, including the *Masterpass Branding Requirements*, wherever card or other payment options are presented to indicate that Masterpass is a checkout option.

If the Masterpass Acceptance Brand 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 Masterpass Acceptance Brand. If following such forty-eight (48) hour period, Mastercard is not able to resolve the issue affecting the functionality of the Masterpass Acceptance Brand, Merchant may disable the Masterpass Acceptance Brand 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 Masterpass Acceptance Brand on the Merchant properties within forty-eight (48) hours of the receipt of notification thereof from Mastercard.

## 3.12 Merchant Advertising

A Merchant may use the Masterpass Marks in advertising material and/or to indicate participation.

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

In marketing or referencing Masterpass, the Merchant or its Merchant Service Providers will portray the Program accurately and fairly and not make any representations, warranties or guaranties inconsistent with any information provided by Mastercard. Except as expressly provided in the *Masterpass Branding Requirements* (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 Masterpass 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 Masterpass Marks in connection with any product or service that is not related to the Masterpass Program, 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 Program are the property of their respective owners, which may or may not be affiliated with, connected to, or sponsored by Mastercard.

## 3.13 Merchant Marks, Product Descriptions and Images

Mastercard may use the Merchant Marks and the Merchant Content (i) as necessary to provide Program-related services, and (ii) to identify the Merchant as participating in all aspects of the Program including related educational, promotional or marketing materials. Customers may use the Merchant Marks and Merchant Content (i) as necessary to provide Program-related services, and (ii) to identify the Merchant as participating in the Program.

## 3.14 Wallet Acceptance Requirements

### 3.14.1 Non-Discrimination

Merchants must accept valid user payment information properly presented from any Wallet. A Merchant must maintain a policy that does not discriminate against a user using one Wallet over another.

### 3.14.2 Specifications

Each Merchant, Merchant Service Provider and Merchant Technology Provider must conduct activities related to their participation in the Program in full compliance with all applicable laws and regulations. Each Merchant, Merchant Service Provider and Merchant Technology

Provider must conduct all activity and otherwise operate in a manner that is financially sound and so as to avoid risk to Mastercard and to other participants in the Program.

A Merchant and its Merchant Service Providers must comply with the Merchant Specifications. Mastercard reserves the right to update or modify these Merchant 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 Program, it must test each to ensure that it operates properly with the Merchant 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 Section 3.11.

### 3.14.3 Updates

Mastercard may make modifications, updates or upgrades to the Masterpass Network, Program, or related Specifications. Each Merchant, its Merchant Service Provider and/or Merchant Technology Providers must upgrade to the latest version of the Masterpass Acceptance Brand and Specifications within six (6) months from the release of such Masterpass Acceptance Brand and/or Specifications. Notwithstanding the foregoing, each Merchant will test and, if necessary, promptly modify its integration and/or any Masterpass-connected websites or other e-commerce applications, at its own expense, to ensure continued Masterpass acceptance using the then-current version of the Specifications and the Program. Except for reasons of security or to address an outage, neither Merchants nor their Merchant Service Providers shall not 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 Masterpass Acceptance Brand and Specifications.

### 3.14.4 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 Masterpass 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.

### 3.14.5 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 a Wallet without the express written consent of Mastercard except where such collection is specifically required by the *Mastercard Rules* or other networks' rules. A Merchant and its Merchant Service Provider(s) must not store CVV Data at any time.

### 3.14.6 Implementing Checkout Postback

A Merchants and/or their Merchant Service Providers shall implement checkout postback expressly as described in the Specifications without modification and shall apply it to every Transaction and transactions with other payment networks conducted via a Wallet.

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

### 3.14.7 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.

## 3.15 Masterpass Prohibited Practices

### 3.15.1 Merchant Acceptable Use Requirements

Merchants may not directly or indirectly engage in or facilitate any action that is illegal or that, in Mastercard's sole discretion and whether or not addressed elsewhere in the Standards (including Section 5.11.7 of *Mastercard Rules*), damages or may damage Mastercard's goodwill or reputation or reflect negatively on any Masterpass Mark. Upon request of Mastercard, Merchants will promptly cease engaging in or facilitating any such action.

Failure to comply adversely affects the Masterpass Mark and all of Mastercard's Customers and undermines the integrity of the Masterpass Network. Mastercard reserves the right to take any corrective action that it deems appropriate, including suspending or restricting the Merchant's and their Merchant Service Providers' participation in the Program, requiring the removal of the Masterpass Acceptance Brand, or any other corrective action, including the imposition of financial assessments on the Acquirer.

### 3.15.2 Minimum/Maximum Transaction Amount Prohibited

Except as expressly permitted by law, a Merchants must not require, or indicate that it requires, a minimum or maximum transaction amount to accept transaction information from a Wallet.

### 3.15.3 Transaction Processing without Confirmation Prohibited

Except as expressly provided in the Specifications, a Merchants must not treat a user's request to use payment information stored in his or her Wallet as confirmation to finalize a checkout.

Except as expressly provided in the Specifications, a Merchant must provide users an opportunity to review their purchase after being returned to the Merchant from the Wallet. No authorization requests should be submitted without user confirmation of the transaction.

## 3.16 Merchant Not to Charge Fees

A Merchant may not charge any fees to a user for his/her use of the Masterpass Network, whether on a per transaction or other basis. Notwithstanding the foregoing, a Merchant is free to charge any fees for the underlying purchase transaction to the extent permitted by the payment network/brand associated with the purchase transaction.

## 3.17 Existing Network Requirements

Participation in the Program 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.

## 3.18 PCI Compliance

Merchants must at all times be, or instead Merchant Service Providers must ensure that all Merchants for which they are performing Program-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.

## 3.19 Merchant Service Provider Agreement with Merchants

A Merchant Service Provider may only enable a Merchant to participate in the Program and become a Merchant if (i) it has entered into an agreement with such Merchant regarding the Program-related services, and (ii) it has been provided by each Merchant with all necessary power and authority to enable Program-related services for such Merchant. In such agreement with each Merchant, the Merchant Service Provider must obligate such Merchant to be bound by these *Masterpass Operating Rules*, 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 *Masterpass Operating Rules*, including without limitation any violation of the *Mastercard Rules*; (b) a Merchant's use of the services; (c) 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 (d) any Transaction initiated by a Merchant using payment information provided to the Merchant Service Provider by the services."

A Merchant's receipt of Program-related services from or through a Merchant Service Provider, including connection to the Masterpass Network and display of the Masterpass Acceptance Brand or other Masterpass Marks, regardless of whether receives such services pursuant to an agreement with the Merchant Service Provider, subjects the Merchant Service Provider and the Customer(s) (as defined under the *Mastercard Rules*) by which such Merchant Service Provider is or should be registered with Mastercard to the indemnification and other obligations as set forth in the Standards, including without limitation these *Masterpass Operating Rules*.

## 3.20 Merchant Service Provider Obligations

A Merchant Service Provider that is, on behalf of one or more Acquirers, providing Program-related services to Merchants must:

1. Provide accurate information to Mastercard regarding the Merchants that are implemented to display the Masterpass Acceptance Brand;
2. Provide and maintain at its cost any necessary items required for its own access, on behalf of Merchants, to Masterpass;
3. Not use the Masterpass Network, and shall ensure each Merchant does not to use the Masterpass Network, in any manner that adversely affects the Masterpass Network 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 Standards and all applicable laws and regulations in connection with providing Program-related services to Merchants, and ensure each Merchant complies and will continue to comply with all Standards and applicable laws and regulations in connection with its access and use of the Masterpass Network.

## 3.21 Privacy and Data Protection; Data Usage

### 3.21.1 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 participation in the Program. 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.

### 3.21.2 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 Masterpass, a **"Merchant Security Incident"**), (d) ensure the proper disposal of Personal Data, and (e) regularly test or otherwise monitor the effectiveness of the safeguards.

### 3.21.3 Security Incidents

(a) 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 Masterpass Express program that may result in such incidents.

(b) 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.

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

### 3.21.4 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 Program 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.

### 3.21.5 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 Program 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 Program 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.

### 3.21.6 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 Program 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 3.21.16 and shall prohibit its subcontractors to Process Personal Data other than as instructed.

### 3.21.7 Data Transfers

Personal Data processed in connection with the Program 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 sections B3 and C5 of these Masterpass Operating Rules.

### 3.21.8 Merchant Use

Unless a Merchant or its Merchant Service Provider provides notice and receives the express consent of the user, it may not 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 participation in the Program. 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 participation in the Program will remain the property of Mastercard. Notwithstanding the foregoing, Merchants may not retain, track, monitor, store or otherwise use Personal Data regarding the user for the purpose of, or in any way that results in, bypassing the Program 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 participation in the Program 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 participation in the Program. 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 *Masterpass Operating Rules*, and agree to comply with such obligations.

### 3.21.9 Merchant Service Provider Use

A Merchant Service Provider may only retain, track, monitor, store or otherwise use Personal Data in accordance with its provision of Services to a Merchant, or to a Customer, and in compliance with these *Masterpass Operating Rules* (including, for the avoidance of doubt, in accordance with applicable law, all applicable privacy policies including those of a Merchant and/or Issuer (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 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 Program-related services, including implementing and/or managing the Masterpass Acceptance Brand 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.

### 3.21.10 Device Scanning and Wallet Selector

Merchants may integrate the Masterpass Materials and technology required for device scanning and display of the wallet selector view, where supported by the operating system of the user's device.

### 3.21.11 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 Program-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 Program (including by developing new product features and services; managing communications; determining the effectiveness of advertising; analyzing Program related products, services and websites; facilitating the functionality of our websites; and performing accounting, auditing, billing, reconciliation and collection activities);
4. Assist a Customer or its Merchant Service Provider in the provision of products, services or Program features incorporated into its Wallet;
5. 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;
6. For preparing and furnishing compilations, analyses and other reports of aggregated information in connection with the Program;
7. If and to the extent Merchant integrates the Mobile Checkout SDK, to facilitate mobile application device scanning to identify each Wallet on a consumer's mobile device and present information from each Wallet, including payment cards registered in such wallet and shipping address, in the Mobile Checkout View, following the Consumer pressing the "Buy With Masterpass" button in the Merchant's mobile application as more fully described in Section 3.21.10;
8. Enforce these *Masterpass Operating Rules*;
9. Comply with applicable legal requirements and industry standards and Mastercard policies; and
10. 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 Program, the Merchant and its Merchant Service Providers shall only use such Personal Data for the purposes permitted by such privacy notice and otherwise in compliance with all applicable law and regulations.

## 3.22 Provision and Use of Information

### 3.22.1 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.

### 3.22.2 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.

### 3.22.3 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 Masterpass Program; 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 Masterpass Program.

### 3.22.4 Confidential Information

A Merchant or a Merchant Service Provider may receive information (whether written, oral, electronic, or otherwise) as part of participation in the Masterpass Program relating to Mastercard or to the Masterpass Program 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 participation in the Masterpass Program; and (c) it will not otherwise disclose Confidential Information to any individual, company, or other third party.

## 3.23 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.

## 3.24 Integrity of Brand and Network

In connection with the Program, 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 Standards, damages or may damage the goodwill or reputation of Mastercard or of any Masterpass 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 Program, 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 Masterpass Network. Specific obligations will be defined in the Masterpass Materials.

## 3.25 Export

Merchants and Merchant Service Providers shall not import or export any of the Masterpass Materials without first obtaining Mastercard's written approval. If so permitted to import or export Masterpass Materials, then Merchants and Merchant Service Providers shall comply with all foreign and U.S. export and import regulations applicable with respect to the Masterpass Materials.

## 3.26 Indemnification

The Merchant, its Merchant Service Providers and Merchant Technology 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, its Merchant Service Providers' and Merchant Technology Providers' obligations set forth in these *Masterpass Operating Rules*, including without limitation any violation of Mastercard's policies; (b) wrongful or improper use of the Program; (c) 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 Program on the Merchant's behalf; (d) 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 Program; (e) any dispute with a user relating to any product or service made available for purchase by Merchant in connection with the Program; (f) any personal injury, product liability or property damage related to any product or service made available for purchase by Merchant in connection with the Program; and (g) 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 Program.

## 3.27 Disclaimer

THE MASTERPASS PROGRAM AND MASTERPASS 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 MASTERPASS MATERIALS, THE PROGRAM 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 MASTERPASS MATERIALS, THE PROGRAM, 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.

## 3.28 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 PROGRAM OR TO ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE PROGRAM (INCLUDING THE INABILITY TO USE THE PROGRAM), THESE *MASTERPASS OPERATING RULES*, THE MASTERPASS MATERIALS, ANY APPLICATION, MERCHANT MARKS OR MERCHANT CONTENT, ANY ANCILLARY SERVICE, OR ANY SERVICES OR GOODS PURCHASED OR TRANSACTIONS ENTERED INTO THROUGH THE PROGRAM. 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 PROGRAM OR TO ANY THIRD PARTY, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE, PRODUCT LIABILITY OR OTHER THEORY) OR OTHERWISE, EXCEED ONE THOUSAND ($1,000) DOLLARS.

## 3.29 Termination

### 3.29.1 Voluntary Termination

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

### 3.29.2 Suspension or Termination by Mastercard

Mastercard may terminate a Merchant or a Merchant Service Provider's participation in the Program 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 (a) the Merchant or Merchant Service Provider has violated the terms of these *Masterpass Operating Rules* (including any Standards), (b) the Merchant or Merchant Service 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 the 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 the Services to and for each such Merchant listed in such notice.

### 3.29.3 Effect of Termination

Upon termination of a Merchant or Merchant Service Provider's participation in the Program, Mastercard will cease providing any access to the Masterpass Network to the Merchant or Merchant Service Provider, respectively, and all Merchants who receive the access to the Masterpass Network through the Merchant Service Provider, and the Merchant Service Provider and each Merchant's rights to access, use and/or participate in the Program (and any other rights) shall immediately cease. WITHOUT LIMITING SECTION 3.28 HEREOF, MASTERCARD WILL NOT BE LIABLE TO THE MERCHANT SERVICE PROVIDER OR ANY MERCHANT FOR ANY TERMINATION OR SUSPENSION OF ACCESS TO THE MASTERPASS NETWORK, WHETHER UPON TERMINATION OF THE MERCHANT SERVICE PROVIDER'S PARTICIPATION THE PROGRAM 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 MASTERPASS NETWORK.

## 3.30 Choice of Laws

The substantive laws of the State of New York govern all disputes involving Mastercard, the Standards, and/or the Merchant's or Merchant Service Provider's participation in the Program without regard to conflicts. Any action initiated by a Merchant or Merchant Service Provider regarding and/or involving Mastercard, the 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 Standards are construed under, and governed by, the substantive laws of the State of New York without regard to conflicts.

# Chapter 4 Europe Region Variations

## Organization of this Chapter

The Standards in this Chapter 4 are variances and additions to the global *Masterpass Operating Rules* in Chapters 1 to 3, and apply to the Europe Region only. Refer to Appendix A of the *Mastercard Rules* for the Europe Region geographic listing.

## SUBSECTION A

### A.1 Choice of Laws

Sections 2.30 and 3.30 of the *Masterpass Operating Rules* are replaced in their entirety by the following:

"**Governing law and Venue.** The *Masterpass Operating Rules* (including any non-contractual obligations or liabilities arising out of them or in connection with them) are governed by and are to be construed in accordance with English law. Each party irrevocably agrees that: (i) the English courts have exclusive jurisdiction to hear and determine any proceedings and to settle any disputes and each party irrevocably submits to the exclusive jurisdiction of the English courts; (ii) any proceedings must be taken in the English courts; (iii) any judgment in proceedings taken in the English courts shall be conclusive and binding on it and may be enforced in any other jurisdiction. Each party also irrevocably waives (and irrevocably agrees not to raise) any objection which it might at any time have on the ground of *forum non conveniens* or on any other ground to proceedings being taken in the English courts. This jurisdiction agreement is not concluded for the benefit of only one party.

**Contracts (Rights Of Third Parties) Act.** A person who is not a party to these *Masterpass Operating Rules* has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any provision of these *Masterpass Operating Rules*. This does not affect any right or remedy of a third party which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999."

### A.2 Use of Mastercard Information

Sections 2.21.2 and 3.22.2 of the *Masterpass Operating Rules* is replaced in its entirety by the following:

"Except in the case of Mastercard's willful misconduct or gross negligence (a) Mastercard is not responsible and disclaims any responsibility for the accuracy, completeness, or timeliness of any information disclosed by Mastercard to a Customer, Customer Service Provider, Merchant or Merchant Service Provider and (b) Mastercard makes no warranty, express or implied, including, but not limited to, any warranty of merchantability or fitness for any particular purpose with respect to any information disclosed by or on behalf of Mastercard to any Customer, Customer Service Provider, Merchant or Merchant Service Provider."

### A.3 Suspension or Termination by Mastercard

Section 3.29.2 of the *Masterpass Operating Rules* is replaced in its entirety by the following in the Europe Region:

Mastercard may terminate a Merchant or a Merchant Service Provider's participation in the Program 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, by giving thirty (30) days 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 it has reasonable grounds to believe that (a) the Merchant or Merchant Service Provider has violated the terms of these *Masterpass Operating Rules* (including any Standards), (b) the Merchant or Merchant Service 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 the 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 the Services to and for each such Merchant listed in such notice.

## SUBSECTION B Data Protection – Mastercard-Hosted Wallet: Europe Region only

### B.1 Definitions

1. "Controller" means the entity which jointly with others determines the purposes and the means of the Processing of Personal Data.
2. "Data Subject" means a cardholder, Merchant, or employee of Customer or Mastercard or other natural person whose Personal Data are processed in the context of this Section.
3. "EU Data Protection Law" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the European Economic Area ("EEA") countries (as amended and replaced from time to time).
4. "Europe" means the EEA, Switzerland, Monaco, and the United Kingdom.
5. "GDPR" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).
6. "Mastercard Binding Corporate Rules" (or "Mastercard BCRs") means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available

at https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf.

7. "Mastercard Rules" means the Rules for the Mastercard, Maestro, and Cirrus brands, as available at http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf.
8. "Personal Data" means 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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
9. "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.
10. "Processor" means the entity which processes Personal Data on behalf of a Controller.
11. "Processing of Personal Data" (or "Processing/Process") means 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.
12. "Wallet-related Personal Data" means Personal Data required for providing a digital wallet service that stores cardholders' payment card and shipping information such as name, surname, email address, phone number, Payment Card Account Number (PAN), Billing Address, Shipping Address, Mobile Phone Number, Email Address, IP Address, PAN Card Expiration Date, Card Verification Code (CVC), Security Q&A for Password Verification, Password, Date of Birth, Gender, Payment Card Brand, Preference settings, Loyalty/reward card data, Shopping Cart Data, transaction data.
13. "Regulators" means a public authority responsible for monitoring the application within its territory of the applicable Privacy and Data Protection Laws.

## B.2 Processing of Personal Data

In relation to the Processing of Personal Data in the context of a Mastercard-Hosted Wallet, each Customer and Mastercard act as Controllers for their own purposes.

Mastercard processes data for the purposes of providing a digital wallet service or as otherwise defined in Clause 2.19. Customer processes data for the purposes of authorizing or declining a transaction. Each Customer and Mastercard shall:

B.2.1 Comply with EU Data Protection Law when Processing of Personal Data (Lawfulness of processing).

B.2.2 Rely on a valid legal ground under EU Data Protection Law for each of its own purposes, including obtaining Data Subjects' appropriate consent if required or appropriate under EU Data Protection Law (Legal ground).

B.2.3 Provide appropriate notice to the Data Subjects regarding (1) the Processing of Personal Data for its own purposes, in a timely manner and at the minimum with the elements required under EU Data Protection Law, (2), as appropriate, the existence of Mastercard BCRs (Notice).

B.2.4. Take 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; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed unless a longer retention is required or allowed under applicable law (Accuracy, data minimization and data retention).

B.2.5. Implement appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law (Accountability).

B.2.6 Respond to Data Subject requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, and (f) objection to the Processing in accordance with EU Data Protection Law (Data Subjects' Rights).

B.2.7. Cooperate with each other to fulfil their respective data protection compliance obligations in accordance with EU Data Protection Law (Cooperation).

## B.3 Data Transfers

In relation to the Processing of Personal Data, each Customer and Mastercard for their own purposes in the context of a Mastercard-Hosted Wallet:

B.3.1. Customer may transfer the Personal Data Processed in connection with the Mastercard-Hosted Wallet outside of Europe in accordance with EU Data Protection Law.

B.3.2.Mastercard may transfer the Personal Data Processed in connection with the Mastercard-Hosted Wallet 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 will abide by the Mastercard BCRs when Processing Personal Data for its own purposes in the context of the Mastercard-Hosted Wallet.

## B.4 Data Disclosures

Customer and Mastercard will only disclose Personal Data Processed in the context of the Mastercard-Hosted Wallet 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 Standards. Mastercard will only disclose Personal Data in accordance with the Mastercard BCRs.

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

B.5.1. Customer and Mastercard must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) 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 (d) 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, Customer and Mastercard must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing 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, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Security measures).

B.5.2. Customer and Mastercard 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 (Confidentiality).

B.5.3. Customer and Mastercard must notify a Personal Data Breach that relates to Personal Data Processed in the context of the Service and for which the other is a Controller, without undue delay, and no later than 48 hours after having become aware of a Personal Data Breach, to the other. Customer and Mastercard will assist each other in complying with their obligations to notify a Personal Data Breach. If Customer or Mastercard 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. 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, Customer or Mastercard must communicate the Personal Data Breach to the Data Subject without undue delay (Data Breaches).

B.5.4. Customer and Mastercard will use their best efforts to reach an agreement on whether and how to notify 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 (Cooperation and Documentation in case of Data Breaches).

## B.6 Data Protection and Security Audit

Customer and Mastercard commit to conduct audits on a regular basis to control compliance with EU Data Protection Law, including the security measures provided under B.5, and Mastercard to control compliance with the Mastercard BCRs. Upon prior written request, Customer and Mastercard agree to cooperate and within reasonable time provide each other with: (a) a summary of the audit reports demonstrating its compliance with EU Data Protection Law obligations and these Standards, 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.

## B.7 Liability

Customer and Mastercard agree that they will be held liable towards Data Subjects for the entire damage resulting from a violation of EU Data Protection Law for its purposes. Where Customer and Mastercard are involved in the same Processing and where they are responsible for any damage caused by the Processing, both Customer 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 Customer that part of the compensation corresponding to Customer's part of responsibility for the damage.

### B.8 Applicable Law and Jurisdiction

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

### B.9 Public Authority's or Regulator's Requests

B.9.1. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Customer and Mastercard must immediately inform each other in writing if any Regulator or public authority of any jurisdiction requests disclosure of, or information about, the Personal Data that are processed in connection with a Mastercard-Hosted Wallet.

B.9.2. Customer and Mastercard shall reasonably cooperate with each other in seeking a protective order or other appropriate protection for the Personal Data and in deciding on an appropriate response to that request.

## SUBSECTION C Data Protection – Partner-Hosted Wallet: Europe Region only

### C.1 Definitions

1. "Controller" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.
2. "Data Subject" means a cardholder or Merchant, or other natural person, whose Personal Data are Processed by the Corporation and a Customer.
3. "EU Data Protection Law" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the European Economic Area ("EEA") countries (as amended and replaced from time to time).
4. "Europe" means the EEA, Switzerland, Monaco, and the United Kingdom.
5. "Mastercard Binding Corporate Rules" (or "Mastercard BCRs") means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available at https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf.
6. "Personal Data" means 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 online identifier or to one or more factors specific to the

physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

7. "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.
8. "Processor" means the entity which processes Personal Data on behalf of a Controller.
9. "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.
10. "Processing of Personal Data" (or "Processing/Process") means 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.
11. "Wallet-related Personal Data" means Personal Data required for providing a digital wallet service that stores cardholders' payment card and shipping information such as name, surname, email address, phone number, Payment Card Account Number (PAN), Billing Address, Shipping Address, Mobile Phone Number, Email Address, IP Address, PAN Card Expiration Date, Card Verification Code (CVC), Security Q&A for Password Verification, Password, Date of Birth, Gender, Payment Card Brand, Preference settings, Loyalty/reward card data, Shopping Cart Data, transaction data.

## C.2 Roles of the Parties

For the purpose of the Standards, Customer and Mastercard acknowledge and confirm that:

C.2.1. Customer is a Controller and Mastercard is a Processor for the Processing of Personal Data for the purpose of offering the Partner-Hosted Wallet.

C.2.2. Customer authorizes Mastercard to process, as a Controller, Personal Data for the purposes listed in Clause 2.19 and 3.21.11 of these Masterpass Operating Rules, including for internal research, fraud, security and risk management. Mastercard shall process Personal Data for these purposes in compliance with EU Data Protection Law, the Mastercard BCRs and the Masterpass Operating Rules.

## C.3 Obligations of Customer

In relation to the Processing of Personal Data for the purposes in the context of Partner-Hosted Wallet, each Customer acts as a Controller and that it shall:

C3.1. Comply with EU Data Protection Law when Processing of Personal Data, and only gives lawful instructions to Mastercard (Lawfulness of processing).

C3.2 Rely on a valid legal ground under EU Data Protection Law for each purpose, including obtaining Data Subjects' appropriate consent if required or appropriate under EU Data Protection Law (Legal ground).

C3.3. Provide appropriate notice to the Data Subjects regarding (1) the Processing of Personal Data for the purposes, in a timely manner and at the minimum with the elements required

under EU Data Protection Law, (2) the existence of Processors located outside of Europe and of the Mastercard BCRs, including the Data Subjects' right to enforce the Mastercard BCRs as third-party beneficiaries (by linking to the Mastercard BCRs).

C3.4. Take 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; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed unless a longer retention is required or allowed under applicable law (Accuracy, data minimization and data retention).

C3.5. Implement appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law, including, as appropriate, appointing a data protection officer, maintaining records of processing, complying with the principles of data protection by design and by default and, where required, performing data protection impact assessments and conducting prior consultations with supervisory authorities (Accountability).

C3.6. Respond to Data Subject requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, and (f) objection to the Processing in accordance with EU Data Protection Law (Data Subjects' Rights).

C3.7. Cooperate with Mastercard to fulfill their respective data protection compliance obligations in accordance with EU Data Protection Law (Cooperation).

## C.4 Obligations of Mastercard

Mastercard shall comply with the Mastercard BCRs and EU Data Protection Law when Processing Personal Data for the purposes defined in these *Masterpass Operating Rules* in connection with the Partner-Hosted Wallet, and that it shall:

C4.1. Only Process Personal Data in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in these Standards or agreed by Customer and Mastercard in writing.

C4.2. Promptly inform Customer if, in its opinion, the Customer's instructions infringe EU Data Protection Law, or if Mastercard is unable to comply with the Customers' instructions. If Mastercard is unable to comply with the Customer's instructions, Customer is entitled to suspend the communication of Personal Data and/or terminate the s Program as provided under 4.7.

C.4.3 Cooperate with the Customer in its role as Controller to fulfil its 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 Customer's own obligations and where applicable to help Customer conducting data protection impact assessments or prior consultation with supervisory authorities.

C.4.4. Keep internal records of Processing of Personal Data carried out as a Processor on behalf of Customer.

C.4.5 Assist Customer in fulfilling its obligation to respond to Data Subjects' requests to exercise their rights as provided under EU Data Protection Law and specified under Clause 3.6., and notifies Customer about such requests if Mastercard receives it directly from Data Subject.

C.4.6. Notify the Customer when local laws prevent Mastercard (1) from fulfilling its obligations under these Standards or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by these Standards or the Mastercard BCRs, and (2) from complying with the instructions received from the Customer via these Standards, 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. Customer is responsible for notifying its competent supervisory authority as applicable and required under applicable law.

C.4.7 Upon termination of the Program or upon a request to delete or return Personal Data, Mastercard will, at the choice of Customer, delete, anonymize, or return all the Personal Data to Customer, 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).

## C.5 Data Transfers

Customer authorizes Mastercard to transfer the Personal Data Processed in connection with the Partner-Hosted Wallet 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 shall abide by the Mastercard BCRs when Processing Personal Data for the purposes in the context of the Partner-Hosted Wallet.

## C.6 Sub-Processing

Customer gives a general authorization to Mastercard to process and sub-process Personal Data to internal and external Sub-Processors in the context of the Program under the conditions set forth below and Mastercard, when sub-processing the Processing of Personal Data in the context of the Partner-Hosted Wallet, it shall:

C.6.1. Bind its internal Sub-Processors to respect Mastercard BCRs and to comply with the Customer' instructions.

C.6.2. Require 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 Customer's instructions and with the same obligations as are imposed on Mastercard by these Standards and the Mastercard's BCRs, including sub-processing and audit requirements set forth in Mastercard BCRs.

C.6.3. Remain liable to the Customer for the performance of its Sub-Processors' obligations.

C.6.4. Commit to provide a list of Sub-Processors to Customer upon request.

C.6.5. Inform the Customer of any addition or replacement of a Sub-Processor in a timely fashion so as to give the Customer an opportunity to object to the change or to terminate the

Program before the Personal Data is communicated to the new Sub-Processor, except where the Program cannot be provided without the involvement of a specific Sub-processor.

## C.7 Security of the Processing; Confidentiality; and Personal Data Breach

C.7.1. Customer and Mastercard must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) 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 (d) 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, Customer and Mastercard must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing 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, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Security measures).

C.7.2. Customer and Mastercard 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 (Confidentiality).

C.7.3. Customer and Mastercard must notify a Personal Data Breach that relates to Personal Data Processed in the context of the Partner-Hosted Wallet to each other, without undue delay, and no later than 48 hours after having become aware of a Personal Data Breach. Mastercard will assist Customer in complying with its obligations to notify a Personal Data Breach. Customer will notify, without undue delay and, where feasible, not later than 72 hours after having become aware of it, the competent supervisory authority. 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, Customer must communicate the Personal Data Breach to the Data Subject without undue delay (Data Breaches).

C.7.4. Customer and Mastercard will use their best efforts to reach an agreement on whether and how to notify 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 (Cooperation and Documentation in case of Data Breaches).

## C.8 Data Protection Audit

Upon prior written request by Customer, Mastercard agrees to cooperate and within reasonable time provide Customer with: (a) a summary of the audit reports demonstrating Mastercard's compliance with EU Data Protection obligations under these Standards 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 Customer to request an audit of Mastercard's data protection compliance program by external independent auditors, which are jointly selected by Customer and Mastercard. The external independent auditor cannot be a competitor of Mastercard, and Customer and Mastercard will mutually agree upon the scope, timing, and duration of the audit. Mastercard will make available to Customer the result of the audit of its data protection compliance program.

### C.9 Liability Towards Data Subjects

Customer and Mastercard agree that they will be held liable for violations of EU Data Protection Law towards Data Subjects as follows:

C.9.1. Customer is responsible for the damage caused by the Processing which infringes EU Data Protection Law or these Standards.

C.9.2. When Mastercard acts as a Processor, it will be liable for the damage caused by the Processing only where it has not complied with obligations of EU Data Protection Law specifically directed to Processors or where it has acted outside of or contrary to Customer's lawful instructions. In that context, Mastercard will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

C.9.3. Where Customer and Mastercard are involved in the same Processing and where they are responsible for any damage caused by the Processing, both Customer 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 Customer that part of the compensation corresponding to Customer's part of responsibility for the damage.

### C.10 Applicable Law and Jurisdiction

This Section and the Processing of Personal Data subject to EU Data Protection Law will be governed by the law of Belgium and that any dispute will be submitted to the Courts of Brussels.

## SUBSECTION D Data Protection – Merchant Rules: Europe Region Only

### D.1 Definitions

1. "Controller" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.
2. "Data Subject" means a cardholder or Merchant, or other natural person, whose Personal Data are Processed by the Corporation and a Customer.
3. "EU Data Protection Law" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as

amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the European Economic Area ("EEA") countries (as amended and replaced from time to time).

4. "Europe" means the EEA, Switzerland, Monaco, and the United Kingdom.
5. "GDPR" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).
6. "Mastercard Binding Corporate Rules" (or "Mastercard BCRs") means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available at https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf.
7. "Mastercard Rules" means the Rules for the Mastercard, Maestro, and Cirrus brands, as available at http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf.
8. "Personal Data" means 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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
9. "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.
10. "Processor" means the entity which processes Personal Data on behalf of a Controller.
11. "Processing of Personal Data" (or "Processing/Process") means 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.
12. "Wallet-related Personal Data" means Personal Data required for providing a digital wallet service that stores cardholders' payment card and shipping information such as name, surname, email address, phone number, Payment Card Account Number (PAN), Billing Address, Shipping Address, Mobile Phone Number, Email Address, IP Address, PAN Card Expiration Date, Card Verification Code (CVC), Security Q&A for Password Verification, Password, Date of Birth, Gender, Payment Card Brand, Preference settings, Loyalty/reward card data, Shopping Cart Data, transaction data.

## D.2 Processing of Personal Data

In relation to the Processing of Personal Data, Merchant acts as a Controller for the purpose of participating in the Program and for displaying the Masterpass Checkout Button and shall:

D.2.1. Comply with EU Data Protection Law when Processing of Personal Data (Lawfulness of processing).

D.2.2. Rely on a valid legal ground under EU Data Protection Law for each of its own purposes, including obtaining Data Subjects' appropriate consent if required or appropriate under EU Data Protection Law (Legal ground).

D.2.3 Provide appropriate notice to the Data Subjects regarding (1) the Processing of Personal Data for its own purposes, in a timely manner and at the minimum with the elements required under EU Data Protection Law, (2), as appropriate, the existence of Mastercard BCRs (Notice).

D.2.4. Take 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; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed unless a longer retention is required or allowed under applicable law (Accuracy, data minimization and data retention).

D.2.5. Take into account the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law. Such measures include, as appropriate, appointing a data protection officer, maintaining records of processing, complying with the principles of data protection by design and by default and, where required, performing data protection impact assessments and conducting prior consultations with supervisory authorities (Accountability).

D.2.6. Respond to Data Subject requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, and (f) objection to the Processing in accordance with EU Data Protection Law (Data Subjects' Rights).

D.2.7. Cooperate with each other to fulfil their respective data protection compliance obligations in accordance with EU Data Protection Law (Cooperation).

D.2.8. Process Personal Data in accordance with Clauses 3.21.8 and 3.21.9.

## D.3 Data Transfers

In relation to the Processing of Personal Data for its purposes in the context of a Mastercard-Hosted Wallet Merchant may transfer the Personal Data Processed in connection with the Wallet outside of Europe in accordance with EU Data Protection Law.

## D.4 Data Disclosures

Each Merchant will only disclose Personal Data Processed in the context of the Wallet in accordance with EU Data Protection Law, and in particular it will require the data recipients to protect the data with at least the same level of protection as in these Standards.

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

D.5.1. Merchant must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity,

availability and resilience of processing systems and services; (c) 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 (d) 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, each Merchant must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing 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, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Security measures).

D.5.2. Merchant 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 (Confidentiality).

D.5.3. Merchant must notify a Personal Data Breach that relates to Personal Data Processed in the context of the Program, without undue delay, and no later than 48 hours after having become aware of a Personal Data Breach, to Mastercard. Each Merchant will assist Mastercard in complying with their obligations to notify a Personal Data Breach. Merchant will notify, without undue delay and, where feasible, not later than 72 hours after having become aware of it, the competent supervisory authority. 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, Merchant must communicate the Personal Data Breach to the Data Subject without undue delay (Data Breaches).

D.5.4. Merchant will use their best efforts to reach an agreement on whether and how to notify 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 (Cooperation and Documentation in case of Data Breaches).

## D.6 Data Protection and Security Audit

Merchant commits to conduct audits on a regular basis to control compliance with EU Data Protection Law, including the security measures provided under B.5, and Mastercard to control compliance with the Mastercard BCRs. Upon prior written request, Merchant agrees to cooperate and within reasonable time provide Mastercard with: (a) a summary of the audit reports demonstrating its compliance with EU Data Protection Law obligations and these Standards, 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.

## D.7 Liability

Each Merchant will be held liable towards Data Subjects for the entire damage resulting from a violation of EU Data Protection Law in the context of this Section. Where Merchant and Mastercard are involved in the same Processing and where they are responsible for any damage caused by the Processing, both Merchant 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 Merchant that part of the compensation corresponding to Merchant's part of responsibility for the damage.

### D.8 Applicable Law and Jurisdiction

Merchant agrees that this Section and the Processing of Personal Data subject to EU Data Protection Law will be governed by the law of Belgium and that any dispute will be submitted to the Courts of Brussels.

## SUBSECTION E – Country Variations

The Standards in this Subsection E are variances and additions to the global *Masterpass Operating Rules* and this Chapter 4, and apply in the country specified below.

### E.1 Israel

1. Section 3.30 of the *Masterpass Operating Rules* is replaced in its entirety by the following in Israel, in relation to Merchants and Merchant Service Providers only:

   "**Governing Law; Venue.** The *Masterpass Operating Rules* (including any non-contractual obligations or liabilities arising out of them or in connection with them) are governed by and are to be construed in accordance with Israeli law. Each party irrevocably agrees that: (i) the Israeli courts have exclusive jurisdiction to hear and determine any proceedings and to settle any disputes and each party irrevocably submits to the exclusive jurisdiction of the Israeli courts; (ii) any proceedings must be taken in the applicable Israeli courts; (iii) any judgment in proceedings taken in the Israeli courts shall be conclusive and binding on it and may be enforced in any other jurisdiction. Each party also irrevocably waives (and irrevocably agrees not to raise) any objection which it might at any time have on the ground of forum non conveniens or on any other ground to proceedings being taken in the Israeli courts. This jurisdiction agreement is not concluded for the benefit of only one party."
2. Subsection (a) of Section 3.26 of the *Masterpass Operating Rules* shall be replaced with the following in Israel:

   "…(a) any breach of the Merchant's, its Merchant Service Providers' and Merchant Technology Providers' obligations set forth in these *Masterpass Operating Rules*, including without limitation any violation of Mastercard's policies…"

### E.2 Romania

The following additional rules apply in Romania, in relation to Merchants and Merchant Service Providers only:

"Each party, in full awareness of the contents and nature of the transactions contemplated by these *Masterpass Operating Rules*, hereby assumes the risk of change of the circumstances under which these *Masterpass Operating Rules* are entered into, in accordance with Article

1271 paragraph 3 letter (c) of the Romanian Civil Code, and hereby waives right to raise defences based on hardship (in Romanian: impreviziune)"

For the purposes of Article 1203 of the Romanian Civil Code, each party hereby expressly accepts all clauses in *Masterpass Operating Rules* which (A) provide in favour of the other party (i) the limitation of liability, (ii) the right to unilaterally terminate (in Romanian: denuntare unilaterala) the *Masterpass Operating Rules* or (iii) the right to suspend performing its obligations, or (B) provide to its detriment (i) the forfeiture of rights (in Romanian: decadere din drepturi), (ii) the forfeiture of the benefit of a timeline (in Romanian: decaderea din beneficiul termenului), (iii) the limitation of the right to raise defenses (in Romanian: dreptul de a opune exceptii), (iv) the limitation of the right to contract with third parties, (v) the tacit renewal of the agreement, (vi) the applicable law, or clauses derogating from the rules of court jurisdiction."

## E.3 Russia

1. Section 3.30 of the *Masterpass Operating Rules* is replaced in its entirety by the following in Russia, in relation to Merchants and Merchant Service Providers only:

   "**Governing Law; Venue.** The Masterpass Operating Rules (including any non-contractual obligations or liabilities arising out of them or in connection with them) are governed by and are to be construed in accordance with Russian law. Each party irrevocably agrees that any dispute arising out of or in connection with these *Masterpass Operating Rules* (including any question regarding the existence, scope, validity or termination of these *Masterpass Operating Rules* or any non-contractual obligation or liability arising out of or in connection with them) shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause. There shall be one arbitrator and the appointing authority shall be the LCIA, such appointment to be made by the LCIA in accordance with the Rules. The seat of arbitration shall be London, all hearings shall take place in London, England, and the arbitration proceedings shall be conducted in English."
2. The following applies in Russia, in relation to Merchants and Merchant Service Providers only:

   "Communications will not be distributed in paper unless Mastercard is contacted with a request for a paper version of a particular document. Mastercard reserves the right to charge handling fee for any notices that Mastercard physically mails on request or because any e-mail address fails."

# Chapter 5 United States Region Variations

## Organization of this Chapter

The Standards in this Chapter 5 are variances and additions to the global *Masterpass Operating Rules* in Chapter 1 to 3, and apply to the United States Region only. Refer to Appendix A of the *Mastercard Rules* for the United States Region geographic listing.

### 3.14.8 Routing Choices

Digital Secure Remote Payments ("DSRP") represents a valuable new technology for secure remote payments that Mastercard offers to Merchants (whether directly or through Merchant Service Providers) for free as (a) an incentive to advance the adoption of this technology-enabled payment option; and (b) an incentive to route transactions through Mastercard's systems and networks.

Each Merchant (whether directly or through a Merchant Service Provider acting on the Merchant's behalf) that:

1. agrees to these *Masterpass Operating Rules*;
2. develops a relevant merchant e-commerce point of sale systems that may utilize tokenized payment credentials from Masterpass (whether in-app, online or in another remote environment); and
3. accepts DSRP transactions using such tokenized payment credentials from Masterpass

acknowledges and agrees that such Merchant is choosing to accept the incremental values offered by acceptance of DSRP transactions and tokenized payment credentials from Masterpass, and choosing to route transactions using those credentials to the Mastercard Network. If a Merchant does not want to route to Mastercard in exchange for this incentive, then that Merchant can accept debit card payments in a more traditional interface that also allows for a routing choice.

# 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.