Mastercard Switch Rules

28 November 2023

MCSR

Contents

Summary of Changes, 28 November 2023

This is a summary of the changes that have occurred since the previous publication of the manual.

Chapter number	Rule name	Source or explanation of revisions
Throughout	Updated "Card Acceptor" and "Merchant" to "Acceptor" and "Submerchant" to "Sponsored Merchant," where applicable.	Relates to AN 6475 Revised Standards for International Organization of Standardization Terminology Alignment.

Chapter number	Rule name	Source or explanation of revisions
Chapter 5 Mastercard Scheme-Specific Requirements	5.1.2 Sponsored Merchant Name Information	Removed requirement for full or abbreviated Payment Facilitator name to be three, seven, or 12 characters in length.
	5.1.6 Merchant Country of Origin of Government Controlled Merchant	Added data fields that must be populated with Merchant Country of Origin data.
	5.4.5 Final Authorizations	Added final authorization performance Standards; relates to AN 6934 Revised Standards for Europe Region Final Authorization Clearing Submission Acceleration (see *Authorization Manual* revisions).
	5.4.12 Multiple Clearing Messages	New section; relates to AN 7259 Revised Standards for Multiple Clearing Messages.
	5.7.4.3 Multiple-authorization Installment Billing	In Table 1, changed description of Transaction Type Identifier (TTI) value P10 from Installment-based Repayment to Purchase Repayment; see AN 6779 Revising Transaction Type Identifier for Purchase Repayments.
	5.10.2 Contactless Transactions 5.10.3 Payment Transactions 5.10.4 Electronic Commerce Transactions 5.10.5 Digital Secure Remote Payment Transactions	Data field names updated to align with technical specifications, where applicable. Added credential-on-file POS entry mode values as valid for electronic commerce and for DSRP transactions with digital payment data.

Applicability of Rules in this manual

This manual contains the specifications and other Standards applicable when a Network Participant uses the Network for authorization, clearing and/or settlement of intra-EEA/United Kingdom/Gibraltar Transactions and Intracountry Transactions in the EEA/United Kingdom/Gibraltar.

A Network Participant indicates its agreement to respect these rules in writing and/or by the act of using the Network for authorization, clearing and/or settlement.

The Rules contained in Chapters 1 through 4 apply to all Network Activities; the Rules contained in Chapters 5 through 7 are additional requirements that apply to scheme-specific or Private Label Network Activity.

Chapter 1 Standards and Conduct of Network Activity

This section describes the standards and conduct of network activity.

1.1 Standards

From time to time, Mastercard Switching Services sets Standards governing Network Activity. Mastercard Switching Services has the sole right to interpret and enforce the Standards.

Mastercard Switching Services has the right, but not the obligation, to resolve any dispute between or among Network Participants including, but not limited to, any dispute involving Mastercard Switching Services, the Standards, or the Network Participants' respective Network Activities, and any such resolution by Mastercard Switching Services is final and not subject to appeal, review, or other challenge. In resolving disputes between or among Network Participants, or in applying the Standards to Network Participants, Mastercard Switching Services may deviate from any process in the Standards or that Mastercard Switching Services otherwise applies, and may implement an alternative process, if an event, including, without limitation, an account data compromise event, is, in the sole judgment of Mastercard Switching Services, of sufficient scope, complexity and/or magnitude to warrant such deviation.

Mastercard Switching Services will exercise its discretion to deviate from its Standards only in circumstances that Mastercard Switching Services determines to be extraordinary. Any decision to alter or suspend the application of any process (es) will not be subject to appeal, review, or other challenge.

1.1.1 Variances

A variance is the consent by Mastercard Switching Services for a Network Participant to act other than in accordance with a Standard. Only a Network Participant may request a variance. Any such request must specify the Rules or other Standards for which a variance is sought. The request must be submitted to Mastercard Switching Services in writing, together with a statement of the reason for the request.

1.1.2 Failure to Comply with a Standard

Failure to comply with any Standard adversely affects Mastercard Switching Services and its Network Participants and undermines the integrity of the Network. Accordingly, a Network Participant that fails to comply with any Standard is subject to assessments ("noncompliance assessments") as set forth in the Standards.

In lieu of, or in addition to, the imposition of a noncompliance assessment, Mastercard Switching Services, in its sole discretion, may require a Network Participant to take such action and Mastercard Switching Services itself may take such action as Mastercard Switching Services deems necessary or appropriate to ensure compliance with the Standards and safeguard the integrity of the Mastercard system. In the exercise of such discretion, Mastercard Switching Services may consider the nature, willfulness, number and frequency of occurrences and possible consequences resulting from a failure to comply with any Standard. Mastercard Switching Services may provide notice and limited time to cure such noncompliance before imposing a noncompliance assessment.

Mastercard Switching Services reserves the right to limit, suspend or terminate a Network Participant's access to the Network, if that Network Participant does not comply with any Standards or with any decision of Mastercard Switching Services with regard to the interpretation and enforcement of any Standards.

1.1.3 Noncompliance Categories

From time to time, Mastercard Switching Services may establish programs that address instances of noncompliance with particular Standards. Every instance of noncompliance with a Standard not addressed by such a program falls into at least one of the following three compliance categories.

Category A: Payment System Integrity

Category A noncompliance affects payment system integrity. Mastercard Switching Services has the authority to impose monetary noncompliance assessments for Category A noncompliance. "Payment system integrity" violations include, but are not limited to, failure to protect Card, Account, and Transaction information.

Category B: Visible to Customers

Category B noncompliance addresses conduct that is visible to customers of the Network Participants. Mastercard Switching Services has the authority to impose monetary noncompliance assessments for Category B noncompliance or, in the alternative, may provide notice and a limited time to cure such noncompliance before imposing monetary assessments. "Visible to Customers" violations include, but are not limited to, noncompliance involving the identification of Transactions and identification of the Merchant at the POI.

Category C: Efficiency and Operational Performance

Category C noncompliance addresses efficiency and operational performance. Mastercard Switching Services has the authority to impose monetary noncompliance assessments for Category C noncompliance or, in the alternative, may provide notice and a limited time to cure such noncompliance before imposing monetary assessments. "Efficiency and operational performance" violations include, but are not limited to, noncompliance involving presentment of Transactions within the required time frame, reporting procedures, and the obligation to provide Mastercard Switching Services with requested information.

1.1.4 Noncompliance Assessments

The following schedule pertains to any Standard that does not have an established compliance program. Mastercard Switching Services may deviate from this schedule at any time.

In the following table, all days refer to calendar days and violations of a Standard are tracked on a rolling 12-month basis.

Compliance Category	Assessment Type	Assessment Description
A	Per violation	Up to USD 25,000 for the first violation Up to USD 50,000 for the second violation within 12 months Up to USD 75,000 for the third violation within 12 months Up to USD 100,000 per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction)	Up to USD 2,500 per occurrence for the first 30 days Up to USD 5,000 per occurrence for days 31–60 Up to USD 10,000 per occurrence for days 61–90 Up to USD 20,000 per occurrence for subsequent violations
	Variable occurrence (by number of Cards)	Up to USD 0.50 per Card Minimum USD 1,000 per month per Portfolio No maximum per month per Portfolio or per all Portfolios
B	Per violation	Up to USD 20,000 for the first violation Up to USD 30,000 for the second violation within 12 months Up to USD 60,000 for the third violation within 12 months Up to USD 100,000 per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction)	Up to USD 1,000 per occurrence for the first 30 days Up to USD 2,000 per occurrence for days 31–60 Up to USD 4,000 per occurrence for days 61–90 Up to USD 8,000 per occurrence for subsequent violations

Compliance Category	Assessment Type	Assessment Description
	Variable occurrence (by number of Cards)	Up to USD 0.30 per Card Minimum USD 1,000 per month per Portfolio Maximum USD 20,000 per month per Portfolio Maximum USD 40,000 per month per all Portfolios
C	Per violation	Up to USD 15,000 for the first violation Up to USD 25,000 for the second violation within 12 months Up to USD 50,000 for the third violation within 12 months Up to USD 75,000 per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction)	Up to USD 1,000 per occurrence for the first 30 days Up to USD 2,000 per occurrence for days 31–60 Up to USD 4,000 per occurrence for days 61–90 Up to USD 8,000 per occurrence for subsequent violations
	Variable occurrence (by number of Cards)	Up to USD 0.15 per Card Minimum USD 1,000 per month per Portfolio Maximum USD 10,000 per month per Portfolio Maximum USD 20,000 per month per all Portfolios

1.1.5 Certification

A senior executive officer of each Network Participant must, if requested by Mastercard Switching Services, promptly certify in writing to Mastercard Switching Services the status of compliance or noncompliance with any Standard by the Network Participant.

1.1.6 Review Process

A Network Participant may request that the Chief Franchise Officer of the Corporation review an assessment imposed by Mastercard Switching Services for noncompliance with a Standard. Such a request must be submitted in writing and signed by the Network Participant's principal contact. The request must be postmarked no later than 30 days after the date of the disputed assessment.

Mastercard Switching Services may assess a USD 500 fee to consider and act on a request for review of a noncompliance assessment.

1.1.7 Resolution of Review Request

When a Network Participant requests review of an assessment for noncompliance with a Standard, the Chief Franchise Officer of the Corporation may take such action as he or she deems necessary or appropriate or may elect not to act. The Chief Franchise Officer may delegate authority to act or not to act with respect to any particular matter or type of matter.

If the Chief Franchise Officer or his or her designee elects to conduct further inquiry into the matter, each Network Participant must cooperate promptly and fully. If the Chief Franchise Officer or his or her designee makes a recommendation of action to resolve the matter, such recommendation is final and not subject to further review or other action.

1.2 Suspension and Termination of Access to Network

A Network Participant's access to the Network may terminate in either of two ways: voluntary termination, or termination by Mastercard Switching Services. It may also be temporarily suspended.

1.2.1 Voluntary Termination

A Network Participant may voluntarily terminate its use of the Network by providing 180 days advance written notice and submitting documentation as then required by Mastercard Switching Services. For the termination to be effective, the Network Participant must effectively cease to use the Network for authorization, clearing and settlement.

1.2.2 Suspension or Termination by Mastercard Switching Services

Notwithstanding anything to the contrary set forth in any agreement with a Network Participant, Mastercard Switching Services, in its sole discretion, may suspend or terminate a Network Participant's access to the Network effective immediately and without prior notice, if:

1. The Network Participant 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 Network Participant, such termination to be effective upon the date of the vote or other action; or
2. The Network Participant 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
3. The government or the governmental regulatory authority having jurisdiction over the Network Participant serves a notice of intention to suspend or revoke, or suspends or revokes, the operations or the charter of the Network Participant; or

4. A liquidating agent, conservator, or receiver is appointed for the Network Participant, or the Network Participant is placed in liquidation by any appropriate governmental, regulatory, or judicial authority; or
5. The Network Participant (i) directly or indirectly engages in or facilitates any action or activity that is illegal, or that, in the good faith opinion of Mastercard Switching Services, and whether or not addressed elsewhere in the Standards, has damaged or threatens to damage the goodwill or reputation of Mastercard Switching Services 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 Switching Services, has damaged or threatens to damage the goodwill or reputation of Mastercard Switching Services or of any of its Marks; or
6. The Network Participant fails to timely provide to Mastercard Switching Services information requested by Mastercard Switching Services and that the Network Participant is required to provide pursuant to the Standards.
7. The Network Participant fails to engage in Network Activity for 26 consecutive weeks or materially fails to operate at a scale or volume of operations consistent with the level agreed with Mastercard Switching Services.
8. Mastercard Switching Services has reason to believe that the Network Participant 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 Switching Services may consider the appearance of the Network Participant, 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
9. Mastercard Switching Services has reason to believe that not terminating access to the Network would be harmful to its or the Corporation's goodwill or reputation.

1.2.3 Rights, Liabilities, and Obligations of a Network Participant Following Termination

All of the following apply with respect to a Network Participant following termination of access to the Network:

A Network Participant is not entitled to any refund of dues, fees, assessments, or other payments and remains liable for, and must promptly pay (a) any and all applicable dues, fees, assessments, or other charges as provided in the Standards and (b) all other charges, debts, liabilities, and other amounts arising or owed in connection with the Network Participant's Network Activity, whether arising, due, accrued, or owing before or after termination.

If a Network Participant does not take an action that this Rule or any other Standard or that Mastercard Switching Services otherwise requires, Mastercard Switching Services may take any such required action without prior notice to the Network Participant and on behalf of and at the expense of the Network Participant.

A Network Participant has no right to present records of Transactions effected after the date of termination to any other Network Participant, except as permitted by the Standards.

A Network Participant must, at the option of Mastercard Switching Services, immediately either destroy, or take such steps as Mastercard Switching Services may require, regarding all confidential and proprietary information of Mastercard Switching Services in any form previously received as a Network Participant.

1.3 Conduct of Network Activity

This topic describes the conduct of the Network Activity.

1.3.1 Network Participant Responsibilities

At all times, each Network Participant must:

1. Be entirely responsible for and Control all aspects of its Network Activity, and the establishment and enforcement of all management and operating policies applicable to its Network Activity, in accordance with the Standards;
2. Not transfer or assign any part or all of such responsibility and Control or in any way limit its responsibility or Control;
3. Ensure that all policies applicable to its Network Activity conform to the Standards and comply with all applicable laws and government regulations;
4. Conduct meaningful and ongoing monitoring to ensure compliance with all of the responsibilities set forth in this Rule, and be able to demonstrate such monitoring and compliance upon request of Mastercard Switching Services in accordance with the Standards, including without limitation, the requirements set forth in the Examination and Audit section of these Rules;
5. Maintain a significant economic interest in each of its Network Activity;
6. Engage in Network Activity at a scale or volume of operations consistent with its role as a Network Participant;
7. Promptly update information previously provided to Mastercard Switching Services in the event of a significant change to the accuracy or completeness of any of the information and, separately, upon request of Mastercard Switching Services;
8. Promptly inform Mastercard Switching Services should the Network Participant become unable for any reason to engage in Network Activity in accordance with both the Standards and the laws and government regulations of any country (or any subdivision thereof) in which the Network Participant engages in Network Activity; and
9. Comply with such other requirements as Mastercard Switching Services may establish, in its sole discretion, in connection with Network Activity.

1.3.2 Financial Soundness

Each Network Participant must conduct all Network Activity and otherwise operate in a manner that is financially sound and so as to avoid risk to Mastercard Switching Services and to other Network Participants.

A Network Participant must promptly report to Mastercard Switching Services any materially adverse financial condition or discrepancy or suspected materially adverse financial condition or discrepancy relating to the Network Participant.

The Network Participant must refer such condition or discrepancy to independent certified public accountants or another person or firm satisfactory to Mastercard Switching Services for evaluation and recommendation as to remedial action, and promptly provide to Mastercard Switching Services a copy of such evaluation and recommendation after receipt thereof.

1.3.3 Compliance with Network Activity Responsibilities

From time to time, Mastercard Switching Services may develop means and apply criteria to evaluate a Network Participant's compliance with the requirements set forth in the Conduct of Network Activity section of these Rules. Each Network Participant must fully cooperate with any effort by Mastercard Switching Services and Mastercard Switching Services' representatives to evaluate a Network Participant's compliance with the requirements set forth in the Conduct of Network Activity section of these Rules.

In the event that Mastercard Switching Services determines that a Network Participant is not complying or may not on an ongoing basis comply with the requirements set forth in the Conduct of Network Activity section of these Rules, Mastercard Switching Services may impose special terms upon the Network Participant as Mastercard Switching Services deems necessary or appropriate until each condition or discrepancy is resolved to Mastercard Switching Services' satisfaction so as to enable the Network Participant to be and to remain in full compliance with the requirements set forth in the Conduct of Network Activity section of these Rules, or require the Network Participant to terminate its use of the Network.

1.4 Indemnity and Limitation of Liability

Each Network Participant (each, for the purposes of this Rule, an "Indemnifying Network Participant") must protect, indemnify, and hold harmless Mastercard Switching Services and Mastercard Switching Services' affiliated entities, and each of the directors, officers, employees and agents of Mastercard Switching Services and Mastercard Switching Services' 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 Network Participant, its subsidiaries, or any person associated with the Indemnifying Network Participant or its subsidiaries (including, without limitation, such Indemnifying Network Participant's directors, officers, employees and agents, all direct and indirect parents, subsidiaries, and affiliates of the Indemnifying Network Participant, the Indemnifying Network Participant's Network Participants in connection with Network Activity and/or other business, and the Indemnifying Network Participant's suppliers, including, without limitation, Service Providers, Card production vendors, and other persons acting for, or in connection with, the Indemnifying Network Participant or a Merchant or other entity for which the Indemnifying Network Participant acquires Transactions, or any such Merchant's or entity's

employees, representatives, agents, suppliers or Network Participants, including any Data Storage Entity [DSE]) with respect to, or relating to:

1. Any Network Activities of the Indemnifying Network Participant;
2. Any programs and/or activities of any person associated with the Indemnifying Network Participant and/or its subsidiaries;
3. The compliance or noncompliance with the Standards by the Indemnifying Network Participant;
4. The compliance or noncompliance with the Standards by any person associated with the Indemnifying Network Participant and its subsidiaries;
5. Any other activity of the Indemnifying Network Participant;
6. Direct or indirect access to and/or use of the Network (it being understood that Mastercard Switching Services does not represent or warrant that the Network or any part thereof is or will be defect-free or error-free and that each Network Participant chooses to access and use the Network at the Network Participant's sole risk and at no risk to Mastercard Switching Services);
7. Any other activity and any omission of the Indemnifying Network Participant and any activity and any omission of any person associated with the Indemnifying Network Participant, its subsidiaries, or both, including but not limited to any activity that used and/or otherwise involved any of the Marks or other assets;
8. Any failure of another Network Participant to perform as required by the Standards or applicable law; or
9. Mastercard Europe Switching Service's interpretation, enforcement, or failure to enforce any Standards.

Mastercard Switching Services does not represent or warrant that the Network or any other system, process or activity administered, operated, controlled or provided by or on behalf of Mastercard Switching Services (collectively, for purposes of this section, the "Systems") is free of defect and/or mistake and, unless otherwise specifically stated in the Standards or in a writing executed by and between Mastercard Switching Services and a Network Participant, the Systems are provided on an "as-is" basis and without any express or implied warranty of any type, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose of non-infringement of third party intellectual property rights. IN NO EVENT WILL MASTERCARD EUROPE SWITCHING SERVICES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, FOR LOSS OF PROFITS, OR ANY OTHER COST OR EXPENSE INCURRED BY A NETWORK PARTICIPANT OR ANY THIRD PARTY ARISING FROM OR RELATED TO USE OR RECEIPT OF THE SYSTEMS, WHETHER IN AN ACTION IN CONTRACT OR IN TORT, AND EVEN IF THE NETWORK PARTICIPANT OR ANY THIRD PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EACH NETWORK PARTICIPANT ASSUMES THE ENTIRE RISK OF USE OR RECEIPT OF THE SYSTEMS.

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, the total liability, in aggregate, of Mastercard Switching Services to a Network Participant and anyone claiming by or through the Network Participant, 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 shall not exceed the total compensation received by Mastercard Switching Services from the Network Participant for the particular use or receipt of the Systems during the 12 months ending on the date that Mastercard Switching Services was advised by the Network Participant of the Systems concern or the total amount of USD 250,000.00, 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.

A payment or credit by Mastercard Switching Services to or for the benefit of a Network Participant 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 Switching Services. A failure or delay by Mastercard Switching Services to enforce any Standard or exercise any right of Mastercard Switching Services set forth in the Standards will not be construed to be a waiver or modification of the Standard or of any of Mastercard Switching Services' rights therein.

1.5 Choice of Laws

These Standards are governed by and construed according to Belgian law, without reference to conflict-of-laws or similar provisions that would mandate or permit the application of the substantive law of any other jurisdiction. Belgian courts have exclusive jurisdiction for the resolution of any dispute relating to the Standards between two Network Participants.

1.6 Examination and Audit

Mastercard Switching Services reserves the right to conduct an examination or audit of any Network Participant and Network Participant information to ensure full compliance with the Standards. Any such examination or audit is at the expense of the Network Participant, and a copy of the examination or audit results must be provided promptly to Mastercard Switching Services upon request.

Further, Mastercard Switching Services, at any time and whether or not a Network Participant is subject to periodic examination or audit or other oversight by banking regulatory authorities of a government, and at the Network Participant's sole expense, may require that Network Participant to be subjected to an examination and/or audit and/or periodic examination and/or periodic audit by a firm of independent certified accountants or by any other person or entity satisfactory to Mastercard Switching Services.

A Network Participant may not engage in any conduct that could or would impair the completeness, accuracy or objectivity of any aspect of such an examination or audit and may not engage in any conduct that could or would influence or undermine the independence, reliability or integrity of the examination or audit. A Network Participant must cooperate fully and promptly in and with the examination or audit and must consent to unimpeded disclosure of information to Mastercard Switching Services by the auditor.

Chapter 2 Network Participant Obligations

This section describes the obligations of network participants.

2.1 Integrity of the Network

A Network Participant must not directly or indirectly engage in or facilitate any action that is illegal or that, in the opinion of Mastercard Switching Services and whether or not addressed elsewhere in the Standards, damages or may damage the goodwill or reputation of Mastercard Switching Services.

Upon request of Mastercard Switching Services, a Network Participant will promptly cease engaging in or facilitating any such action.

2.2 Fees, Assessments, and Other Payment Obligations

Each Network Participant is responsible to timely pay to Mastercard Switching Services all fees, charges, assessments and the like applicable to Network Activity as may be in effect from time to time, including those set forth in the applicable Mastercard Consolidated Billing System Digital Pricing Guide.

If a Network Participant does not timely pay Mastercard Switching Services or any other person any amount due under the Standards, then Mastercard Switching Services has the right, immediately and without providing prior notice to the Network Participant, to assess and collect from that Network Participant, on a current basis as Mastercard Switching Services deems necessary or appropriate, such amount, as well as the actual attorneys' fees and other costs incurred by Mastercard Switching Services in connection with any effort to collect such amount from that Network Participant.

Mastercard Switching Services may assess and collect such amount at any time after the applicable amount becomes due, by any means available to Mastercard Switching Services, which shall specifically include, by way of example and not limitation:

1. The taking or setoff of funds or other assets of the Network Participant held by Mastercard Switching Services;
2. The taking or setoff of funds from any account of the Network Participant upon which Mastercard Switching Services is authorized to draw;
3. The taking of funds being paid by the Network Participant to any other Network Participant; and
4. The taking of funds due to the Network Participant from any other Network Participant.

Each Network Participant expressly authorizes Mastercard Switching Services to take the Network Participant's funds and other assets as authorized by this Rule, and to apply such funds and other assets to any obligation of the Network Participant to Mastercard Switching Services or any other person under the Standards, and no Network Participant shall have any claim against Mastercard Switching Services or any other person in respect of such conduct by Mastercard Switching Services.

Each Network Participant agrees upon demand to promptly execute, acknowledge and deliver to Mastercard Switching Services such instruments, agreements, lien waivers, releases, and other documents as Mastercard Switching Services may, from time to time, request in order to exercise its rights under this Rule.

2.2.1 Taxes and Other Charges

Each Network Participant must pay when due all taxes with respect to its Network Activity charged by any country or other jurisdiction in which the Network Participant conducts such Network Activity.

In the event Mastercard Switching Services is charged taxes or other charges by a country or other jurisdiction as a result of or otherwise directly or indirectly attributable to Network Activity, the Network Participant is obligated to reimburse Mastercard Switching Services the amount of such taxes or other charges. Mastercard Switching Services may collect such taxes or other charges from the settlement account of the Network Participant responsible in accordance with the Standards for the Network Activity that gave rise to the charge.

2.3 Obligation of Network Participant to Provide Information

Each Network Participant must provide Mastercard Switching Services with its current contact information, including mailing addresses, air express/hand delivery addresses, telephone numbers, fax numbers, and e-mail addresses.

2.4 Confidential Information of Network Participants

As used in this Rule 2.4, Confidential Information of Network Participants, the following terms have the meanings as described below.

Term	Definition
Confidential Information	Any information of any nature that comes into the possession or under the control of Mastercard Switching Services, whether temporarily or permanently and whether directly or indirectly, resulting from the Network Activity or any service provided by or product of Mastercard Switching Services and which information is deemed by a person other than Mastercard (including, by way of example and not limitation, a Network Participant) to be confidential information of such person.
Controller	The entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.
Data Subject	A Cardholder, a Merchant, or other natural person or entity whose Personal Data are Processed by Mastercard Switching Services and a Network Participant or a Merchant.

Term	Definition
EU Data Protection Law	The EU General Data Protection Regulation 2016/679 and the e-Privacy Directive 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them in any country in the European Economic Area ("EEA"); their national implementing legislation the UK GDPR and Data Protection Act 2018; the Monaco Data Protection Act; the Swiss Federal Data Protection Act (the "FADP"); and any legislation and/or regulation which amends, replaces, re-enacts or consolidates any of them.
Government Agency	Any competent public or quasi-public authority (including without limitation regulators, local government authorities, law enforcement authorities and national security agencies) of any jurisdiction that may request disclosure of Personal Data Processed in connection with the Network Activity.
Mastercard BCRs	The Mastercard Binding Corporate Rules as approved by the EEA data protection authorities, available on the Corporation's public facing website.
Personal Data	Any information relating to an identified or identifiable individual, including contact information, demographic information, passport number, Social Security number or other national identification number, bank account information, Primary Account Number and authentication information (such as, identification codes, passwords).
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed.
Processor	The entity that Processes Personal Data on behalf of a Controller.
Processing of Personal Data	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 of such data.

Term	Definition
Standard Contractual Clauses or SCCs	With respect to Personal Data to which the GDPR applies, the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, and not including any clauses marked as optional ("EU Standard Contractual Clauses" or "EU SCCs"); With respect to Personal Data to which the FADP applies, the EU Standard Contractual Clauses, provided that any references in the clauses to the GDPR shall refer to the FADP; With respect to Personal Data to which the UK GDPR applies, the International Data Transfer Addendum to the EU SCCs ("UK Addendum"), issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but, as permitted by clause 17 of the UK Addendum, the parties agree to change the format of the information set out in Part 1 of the UK Addendum so that: • the details of the parties in table 1 of the UK Addendum shall be as set out in Annex 1 (with no requirement for signature); • for the purposes of table 2 of the UK Addendum, the first option is selected, and the "Approved EU SCCs" are those incorporated as per the paragraph above; and • the appendix information listed in table 3 of the UK Addendum is set out in Annex 1 and 2.
Sensitive Data	Any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any future revision of EU Data Protection Law.
Third Country	A country where the laws applicable to Personal Data do not offer the same level of protection for such Personal Data as the one set out by EU Data Protection Law.
UK Data Protection Law	The Data Protection Act 2018; the GDPR as amended by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 ('UK GDPR') as relevant; and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) as transposed into UK national law.
Sub-Processor	The entity engaged by the Processor or any further subcontractor to Process Personal Data on behalf of and under the instructions of the Controller.
Transaction-related Personal Data	Personal Data required for authorizing, recording, clearing and settling a Transaction by the Corporation.

Term	Definition
Geographic Scope of Application	The Rule 2.4, Confidential Information of Network Participant applies to Processing of Personal Data, which is subject to the EU Data Protection Law.

2.4.1 Data Uses for Mastercard Switching Services

Mastercard Switching Services will not use, disclose or otherwise Process Transaction-related Personal Data and other Personal Data or Confidential Information provided to it by Network Participants except to the extent that the use, disclosure or Processing is compliant with EU Data Protection Law and Mastercard BCRs, and relies on one of the purposes defined below:

1. For the benefit of, on behalf and upon instruction of the Network Participants supplying the information to support the Network Participants' Program and/or Network Activities;
2. As required for authorization, clearing, and settlement of a Transaction;
3. As may be appropriate to Mastercard Switching Services and Mastercard Switching Services' affiliated entities, staff, accountants, auditors, or counsel for the execution of their respective tasks, including but not limited to auditing, billing, reconciliation and collection activities performed in the context of the services on the Network Participant;
4. For the purpose of processing and/or resolving chargebacks or other disputes;
5. For the purpose of protecting against or preventing actual or potential fraud, unauthorized transactions, claims, or other liability;
6. For the purpose of providing products or services to Network Participants, provided that any Confidential Information or Personal Data provided in such products or services will consist solely of information provided to Mastercard Switching Services by that Network Participant;
7. For preparing internal reports for use by Mastercard Switching Services or any of Mastercard Switching Services' affiliated entities, staff, management, and consultants for the purposes of operating, evaluating, and managing Mastercard Switching Services business;
8. For anonymizing Personal Data to prepare and furnish aggregated and anonymized data reports, compilations, or analysis, provided that such compilations, analysis, or other reports (i) do not identify any Network Participant other than the Network Participant for which the compilation, analysis, or other report is prepared and (ii) do not contain any Personal Data;
9. As may be required by applicable laws and regulations or requested by any judicial process or governmental agency having or claiming jurisdiction over Mastercard Switching Services or Mastercard Switching Services' affiliated entities; or
10. For other purposes for which the Data Subject to whom the Personal Data relates has provided explicit consent.

2.4.2 Processing of Transaction-Related Personal Data

With regard to Transaction-related Personal Data, Network Participants must comply with EU Data Protection Law.

Network Participants act as Controllers with regard to the Processing of Personal Data for the purposes of authorizing, recording, clearing and settling Transactions, and Mastercard Switching Services acts as a Processor for these purposes.

Network Participants acknowledge that Mastercard Switching Services may Process, as a Controller, Personal Data for the purposes listed in Rule 2.4.1 of the Standards and in the Mastercard BCRs in relation to accounting, auditing and billing; fraud, financial crime and risk management; defense against claims, litigation and other liabilities; arbitration and other decisions made for dispute resolution; product development and improvement; internal research, reporting and analysis; anonymization of data to develop data analytics products; and compliance with legal obligations. Mastercard Switching Services represents and warrants that it will process Personal Data for these purposes in compliance with EU Data Protection Law, the Mastercard BCRs and the Standards.

To the extent it acts as Processor, Mastercard Switching Services will: (1) cooperate with Network Participants in their role as Controllers to fulfill their data protection compliance obligations in accordance with EU Data Protection Law; (2) only undertake Processing of Personal Data in accordance with the Network Participants' lawful written instructions and not for any other purposes than those specified in the Standards, and the Mastercard BCRs, or as otherwise agreed in writing; and (3) comply with obligations equivalent to those imposed on the Network Participants as Controllers by the provisions of EU Data Protection Law, including those applicable to Processors and data transfers.

Mastercard Switching Services will notify Network Participants when local laws prevent Mastercard Switching Services from (1) complying with Network Participant's instructions (unless applicable law prohibits such information on important grounds of public interest such as to preserve the confidentiality of a law enforcement investigation), and (2) fulfilling its obligations under the Standards or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by the Standards or the Mastercard BCRs.

2.4.3 Mastercard BCRs

Mastercard Switching Services will abide by the Mastercard BCRs when the Processing of Personal Data is or was subject to EU Data Protection Law.

2.4.4 Data Subject Notice and Legal Grounds for the Processing of Personal.

Network Participants must ensure that the Processing of Personal Data by the applicable Network Participant and Mastercard Switching Services for the purposes provided in Rule 2.4.1, Data Uses for Mastercard Switching Services of this manual, relies on a valid legal ground under EU Data Protection Law, including obtaining Data Subjects' proper consent where required or appropriate under EU Data Protection Law.

Network Participants must ensure that Data Subjects receive appropriate notice, in a timely manner: (1) at the minimum with all the elements required under EU Data Protection Law; (2)

about the existence of Processors located outside of the EEA; and (3) where required and appropriate, about the existence of Mastercard BCRs and Data Subjects' right to enforce the Mastercard BCRs as third-party beneficiaries (by referring to the public version of the Mastercard BCRs).

2.4.5 Data Subject Rights

Network Participants must develop and implement appropriate procedures for handling Data Subjects' requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) portability (e) restriction of Processing, (f) objection, and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them.

To the extent that Mastercard Switching Services acts as a Processor, it will respond in accordance with applicable EU Data Protection Law, and Mastercard Switching Services will assist the relevant Network Participant in complying with its obligations to respond to such requests, including by providing access to Personal Data maintained by Mastercard Switching Services.

2.4.6 Personal Data Accuracy and Data Minimization

Each Network Participant must take reasonable steps to ensure that Personal Data such Network Participant provides to Mastercard Switching Services is: (1) accurate, complete and current; (2) adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed; and (3) 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.

2.4.7 Accountability

Taking into account the nature, scope, context and purposes of the Processing as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, Mastercard Switching Services, Network Participants must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the Processing is performed in accordance with the Standards and EU Data Protection Law, including, as applicable, by appointing a data protection officer, maintaining records of Processing, complying with the principles of data protection by design and by default, performing data protection impact assessments and conducting prior consultations with supervisory authorities. Mastercard Switching Services will cooperate with and assist the Network Participants in fulfilling their own obligations under EU Data Protection Law.

2.4.8 International Data Transfers

Each Network Participant authorizes Mastercard Switching Services to transfer the Personal Data Processed subject to EU Data Protection Law outside of the Europe Region, and in particular into the United States Region and India, 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.

To the extent that Mastercard Switching Services makes any transfer of Personal Data subject to EU Data Protection Law to a Network Participant in a Third Country, the Parties agree that the transfer shall be governed by the EU SCCs, which are hereby incorporated by reference, as though such obligations were set out in full in these Standards, and with the Network Participant's and the Mastercard Switching Services' signature and dating of the relevant Agreement, or other enrollment form, announcement, or any other relevant documents by which Network Participant is bound by these Standards being deemed to be the signature and dating of the EU SCCs. The EU SCCs are completed as follows: the Parties conclude Module Four (processor-to-controller) of the EU SCCs.

- The "data exporter" is Mastercard Switching Services; the "data importer" is Network Participant;
- Clause 16 (Governing law): the clauses shall be governed by the laws of Belgium;
- The information as required by Annex I of the SCCs is as set out in Annex 1 of this section.

The Parties conclude the UK Addendum for transfers of Personal Data subject to the UK Data Protection Act from Corporation to Customer in a country that is not subject to a UK adequacy decision. The UK Addendum is hereby incorporated by reference.

If the Corporation's compliance with EU Data Protection Law applicable to international data transfers is affected by circumstances outside of the Corporation's control, including if a legal instrument for international data transfers is invalidated, amended, or replaced, then Customer and the Corporation will work together in good faith to reasonably resolve such non-compliance.

In the event the Corporation is compelled to comply with a Disclosure Request and such disclosure causes Customer to breach EU Data Protection Law, Customer represents and warrants that it will not hold the Corporation liable for such disclosure. Customer further agrees that - to the greatest extent authorized by applicable law - it will not revoke or amend its instruction to Process Personal Data unless strictly required by EU Data Protection Law. Any amendments to Customer's instructions to Process Personal Data, such as where necessary to ensure the continued compliance with EU Data Protection Law, must be agreed by both parties in writing prior to taking effect.

2.4.9 Sub-Processing

To the extent Mastercard Switching Services acts as a Processor, Network Participant gives a general authorization to Mastercard Switching Services to Process and sub-Process Personal Data to internal and external Sub-Processors in the context of the Network Participant's Activities under the conditions set forth below and when sub-processing the Processing of Personal Data in the context of the Network Participant's Activities, Mastercard Switching Services:

- Binds its internal Sub-Processors to respect the Mastercard BCRs and to comply with the Network Participant's instructions.
- Requires its external Sub-Processors, via a written agreement, to comply with the requirements of Europe Data Protection Law applicable to Processors and data transfers, with the Network Participant's instructions and with the same obligations as are imposed on

Mastercard Switching Services by the Rules and Mastercard's BCRs, including sub-Processing and audit requirements set forth in Mastercard's BCRs.

- Remains liable to the Network Participant for the performance of its Sub-Processors' obligations.
- Commits to provide a list of Sub-Processors to Network Participant upon request.
- Will inform Network Participant of any addition or replacement of a Sub-Processor in a timely fashion so as to give Network Participant an opportunity to object to the change before the Personal Data is communicated to the new Sub-Processor.

Government Requests for Personal Data

Where the Mastercard Switching Services is requested to disclose Personal Data to a Government Agency that the Mastercard Switching Services is Processing, Mastercard Switching Services will only comply with such request in accordance with the Mastercard BCRs and EU Data Protection Law.

Where Mastercard Switching Services is acting as a Processor, it shall refer the Government Agency to the Network Participants, unless Mastercard Switching Services is prohibited from doing so.

2.4.10 Security, Confidentiality and Data Protection Audit

In accordance with the Standards and EU Data Protection Law, Mastercard Switching Services, Network Participants 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.

In assessing the appropriate level of security, Mastercard Switching Services, Network Participants must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the 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.

Mastercard Switching Services, Network Participants 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, as applicable, Processes Personal Data in accordance with the Network Participants' instructions.

Upon prior written request by the Network Participants, to the extent it acts as Processor and subject to the strictest confidentiality obligations, Mastercard Switching Services will, within reasonable time, provide to the relevant Networks Participants with: (a) a summary of the audit reports demonstrating Mastercard Switching Services' compliance with EU Data Protection Law and the Mastercard BCRs, after redacting any confidential or commercially sensitive information; and (b) a 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 Switching Services will allow such Network Participants to request an audit of Mastercard's data protection compliance program by external independent auditors, which are jointly selected by Mastercard Switching Services and Network Participants. The external independent auditor cannot be a competitor of Mastercard Switching Services, and Mastercard Switching Services and the Network Participants will mutually agree upon the scope, timing, and duration of the audit. Mastercard Switching Services will make available to the Network Participants the result of the audit of its data protection compliance program.

2.4.11 Personal Data Breaches

Where Mastercard Switching Services acts as a Processor, it will inform Network Participants without undue delay, and no later than 48 hours after having become aware of it, of a Personal Data Breach. Mastercard Switching Services will assist Network Participants in complying with their own obligations to notify a Personal Data Breach.

2.4.12 Termination and Mandatory Retention

To the extent that Mastercard Switching Services acts as a Processor, upon Termination of the provision of Mastercard Switching Services or upon requests to delete or return Personal Data, Mastercard Switching Services will, at the choice of the relevant Network Participant, delete, anonymize, or return all the Personal Data to such Network Participant, and delete or anonymize existing copies unless applicable law prevents it from returning or destroying all or part of the Personal Data or requires storage of the Personal Data in which case Mastercard Switching Services will protect the confidentiality of the Personal Data and will not actively Process the Personal Data.

2.4.13 Liability for EU Data Protection Law Violations

Where a Network Participant, or Mastercard Switching Services act as a Controller, they are responsible for the damage caused by the Processing of Personal Data which infringes the Standards and EU Data Protection Law.

To the extent that Mastercard Switching Services acts as a Processor, it will only 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 or contrary to Network Participant's lawful instructions. Mastercard Switching Services will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where one or more Network Participants and/or Mastercard Switching Services are involved in the same Processing and where they are responsible for any damage caused by the Processing, each may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Mastercard Switching Services paid full compensation for the damage suffered, it is entitled to claim back from the Network Participants involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage.

2.4.14 Use of Mastercard Switching Services Information by a Network

Mastercard Switching Services is not responsible for and disclaims any responsibility for the accuracy, completeness, or timeliness of any information disclosed by Mastercard Switching Services or its to a Network Participants; and Mastercard Switching Services 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 the Mastercard Switching Services to any Network Participant directly or indirectly. Each Network Participant assumes all risk of use of any information disclosed directly or indirectly to a Network Participant or to any participant in a Network Participant's Network Activity by or on behalf of Mastercard Switching Services.

2.4.15 Confidential Information of Mastercard Switching Services

A Network Participant must not disclose confidential information of Mastercard Switching Services or its parents, subsidiaries, and affiliates (herein collectively referred to as Mastercard) except:

1. On a need-to-know basis to the Network Participant's staff, accountants, auditors, or legal counsel subject to standard confidentiality restrictions, or
2. As may be required by any court process or governmental agency having or claiming jurisdiction over the Network Participant, in which event the Network Participant must promptly provide written notice of such requirement to the Mastercard Switching Services, and to the extent possible, the Network Participant must seek confidential treatment by the court or agency.

The obligation set forth herein continues following the termination of a Network Participant's Mastercard License.

Information provided to a Network Participant by Mastercard is deemed confidential unless otherwise stated in writing.

A Network Participant may use confidential or proprietary information and/or trade secrets of Mastercard solely for the purpose of carrying out its Network Activities.

2.4.15.1 Network Participant's Evaluation of Mastercard Technology

From time to time, Mastercard Switching Services may disclose certain specifications, designs and other technical information or documentation developed by Mastercard (as defined in Rule 2.4.15) (hereinafter the "Mastercard Specifications") to a Network Participant, solely for the purpose of the Network Participant's evaluation of such Mastercard Specifications. Any such disclosure is subject to the following:

1. Each Network Participant to which Mastercard Switching Services disclosed any Mastercard Specifications is given a non-exclusive, limited, nontransferable, non-sublicenseable right to reproduce and use such Mastercard Specifications solely for the limited purpose of the Network Participant's internal evaluation. A Network Participant may implement prototypes based on the Mastercard Specifications for its internal evaluation purposes in furtherance of such limited purpose, but the Network Participant may not distribute, license, offer to sell, supply or otherwise provide, demonstrate, or otherwise transfer or

disclose, to any third party, any Mastercard Specifications, or any implementation of any Mastercard Specifications.

2. Mastercard Switching Services does not convey, and no Network Participant obtains, any rights or license in or to the Mastercard Specifications or any other intellectual property of Mastercard as a result of this section, other than as expressly set forth in this section. All rights not expressly granted to a Network Participant with respect to the Mastercard Specifications are retained by Mastercard.
3. Each Network Participant must treat the Mastercard Specifications and all implementations of the Mastercard Specifications as Confidential Information of Mastercard subject to section 2.4.15.
4. Notwithstanding any other Standard relating to a Network Participant's use of Service Providers, a Network Participants may not use any Service Providers in connection with the Network Participant's exercise of its rights under this section, without the express prior written consent of the Mastercard Switching Services, which consent may be withheld or conditioned on other terms and conditions, in Mastercard Switching Services' sole discretion.

2.5 Cooperation

A Network Participant must fully cooperate with Mastercard Switching Services and all other Network Participants in the resolution of disputes.

A Network Participant, to the best of its ability, must provide requested investigative assistance to any other Network Participant.

Chapter 3 Settlement and Related Obligations

This section describes the settlement and related obligations.

3.1 Net Settlement

A Network Participant that uses the Network for clearing of Transactions is required to net settle in accordance with the settlement Standards. However, an Acquirer and an Issuer may, with respect to a particular Transaction, agree to settle directly between themselves pursuant to a bilateral agreement.

Standards describing net settlement and bilateral agreement rights and obligations are set forth in the Settlement Manual.

3.1.1 Currency Conversion

Mastercard Switching Services converts Transactions processed through use of the Network into the applicable settlement currency. The Acquirer must submit each Transaction in the currency in which it occurred.

If two Network Participants elect not to settle a Transaction by using the Network and instead elect to settle directly between themselves in accordance with a bilateral agreement, any Transaction currency that Mastercard Switching Services supports is acceptable for settlement.

3.1.2 Settlement Finality

Mastercard Switching Services determines the net obligations of the Network Participants under the Standards. Network Participants' net obligations are calculated by Mastercard Switching Services' proprietary small value clearing systems and are based upon accepted financial messages submitted by the Network Participants to the Network.

Financial messages are considered irrevocable, by Network Participants, upon completion of the clearing system cutoff. However, in accordance with the Standards, Network Participants may submit a separate financial message to offset a previously submitted financial message.

Mastercard Switching Services subsequently creates instructions, reflecting the Network Participants' end-of-day net obligations, which result in the assumption or discharge of payment obligations between Network Participants. These instructions are effected by Network Participants and the settlement agents of Mastercard Switching Services. Settlement finality of the transfer order is determined by the rules of the national payment system in which the funds transfer is executed.

3.1.2.1 Cooperation with Government Authorities

Each Network Participant agrees and acknowledges that, for the purposes of administering the Network, Mastercard Switching Services may from time to time co-operate (by sharing of information or otherwise) with:

1. The European Central Bank ("ECB");
2. The National Bank of Belgium ("NBB");
3. Bank of England ("BoE"); and

4. Any authority, body or person having responsibility for any matter arising out of, or connected with, the default of a Network Participant.

3.1.2.2 Reconciliation

It is the responsibility of each Network Participant to reconcile the totals and Transactions provided by the Network to its own internal records on a daily basis.

For more information on reconciliation, refer to the *Global Clearing Management System Reference Manual*.

Chapter 4 Connecting to the Network and Authorization Routing

This section describes connecting to the network and authorization routing.

4.1 Connecting to the Network

Before switching Transactions and on an ongoing basis thereafter, the Network Participant must perform testing and obtain any necessary certifications of its equipment, procedures, and Network connections as may be required by Mastercard Switching Services to ensure compatibility with its technical specifications then in effect.

Each Network Participant must establish and maintain, at its own expense, a data processing facility that is capable of receiving, storing, switching, and communicating any Transaction sent to or received from the Network, and may connect at least one data processing facility directly to the Network. Such facility may be established and maintained by the Network Participant's parent, its wholly-owned subsidiary, or an entity that is wholly owned, directly or indirectly, by the Network Participant's parent, or with the prior written agreement of Mastercard Switching Services, by the Network Participant's designated third party agent.

4.2 Routing Instructions and System Maintenance

Each Network Participant must:

1. Submit to Mastercard Switching Services completed institution routing table (IRT) and institution definition file (IDF) input documents no later than five business days prior to the requested effective date of live switching via the Network.
2. Notify Mastercard Switching Services of any routing updates at least five business days before the effective date of the change. Expedited maintenance may be performed within two business days of such notice.
3. Notify Mastercard Switching Services of any scheduled downtime at least 24 hours in advance.

Chapter 5 Mastercard Scheme-Specific Requirements

This section describes the requirements for Mastercard scheme-specific information.

5.1 Transaction Message Data

This topic describes specifications relating to transaction message data.

5.1.1 Acceptor Address Information

The Acquirer must transmit the generally accepted location, city, and country of the Terminal or website in DE 43 (Acceptor Name/Location), substantially the same as it appears on any Transaction receipt provided.

5.1.2 Sponsored Merchant Name Information

The Acquirer must ensure that a Transaction conducted by a Sponsored Merchant includes the names of both the Payment Facilitator and the Sponsored Merchant in DE 43 (Acceptor Name/Location), subfield 1 (Acceptor Name).

The Payment Facilitator name, in full or in abbreviated form, followed by "*" and the Sponsored Merchant name.

5.1.3 Payment Facilitator ID and Sponsored Merchant ID

An Acquirer that uses a Payment Facilitator must populate the Payment Facilitator field with a Payment Facilitator (PF) ID in all Transaction messages as follows. The PF ID must match the Company ID provided during Payment Facilitator registration or will be provided directly by the Corporation.

1. DE 48 (Additional Data: Private Use), subelement 37 (Additional Acceptor Data), subfield 1 (Payment Facilitator ID) of Authorization Request/0100 messages; and
2. PDS 0208 (Additional Acceptor Data), subfield 1 (Payment Facilitator ID) of First Presentment/1240 messages.

An Acquirer that uses a Payment Facilitator must populate the Sponsored Merchant field with a Sponsored Merchant ID in all Transaction messages as follows. The Sponsored Merchant ID must match the Sponsored Merchant ID supplied by the Acquirer or Payment Facilitator.

1. DE 48 (Additional Data: Private Use), subelement 37 (Additional Merchant Data), subfield 3 (Sponsored Merchant ID) of Authorization Request/0100 messages; and
2. PDS 0208 (Additional Acceptor Data), subfield 2 (Sponsored Merchant ID) of First Presentment/1240 messages.

5.1.4 ATM Terminal Information

The Acquirer of an ATM Transaction must transmit the ATM owner name and ATM location address in DE 43 and the unique ATM Terminal identification information in DE 41 (Acceptor Terminal ID) of each Transaction message.

An Acquirer and any Service Provider performing ATM Transaction switching services must also identify itself using a unique number, which is assigned by the Network.

5.1.5 Independent Sales Organization

An Acquirer that uses an Independent Sales Organization (ISO) must populate the ISO field with an ISO identification number (ID) in all Transaction messages arising from a Merchant, Sponsored Merchant, or ATM owner receiving or otherwise benefiting from the Program Service performed by that ISO.

The ISO ID must match the Company ID provided during ISO registration, and which may be found in the Business Administration tool using Mastercard Connect®. The ISO identifier must appear in the following fields:

- DE 48 (Additional Data: Private Use), subelement 37 (Additional Acceptor Data), subfield 2 (Independent Sales Organization ID) of Authorization Request/0100 messages; and
- PDS 0209 (Independent Sales Organization ID) of First Presentment/1240 messages.

5.1.6 Merchant Country of Origin of Government Controlled Merchant

Each Authorization Request/0100, Authorization Advice/0120, and Reversal Advice/0400 message for a Transaction conducted by a Government Controlled Merchant must include the Merchant Country of Origin for that Government Controlled Merchant, whether such country is the same as or different from the country in which the Merchant is located or the Transaction occurs. The Merchant Country of Origin must be provided in DE 48 (Additional Data: Private Use), subelement 37 (Additional Acceptor Data), subfield 4 (Home Country ID) of Authorization Request/0100 and Authorization Advice/0120 messages, and in PDS 0213 (Home Country ID) in First Presentment/1240 messages.

5.2 Authorization Routing—Mastercard POS Transactions

On an ongoing basis, an Acquirer of Mastercard POS Transactions must recognize all active Mastercard bank identification numbers (BINs) for purposes of obtaining Transaction authorizations, and obtain such authorizations on behalf of each of its Merchants as the Standards require.

If the Acquirer uses Account range files provided by Mastercard Switching Services for this purpose, such files must be loaded and functioning on the Acquirer's host system and available to its Merchants for use within six calendar days from the date that each updated file is distributed. Upon receipt of an updated Account range file from Mastercard Switching Services, an Acquirer must confirm via an acknowledgment file that it updated its host systems accordingly. Alternatively, the Acquirer may submit all authorization requests containing an Account number with a BIN in either the 222100 to 272099 range or the 510000 to 559999 range to the Network for routing to the Issuer.

5.3 Authorization Routing—Maestro POS, ATM Terminal, and PIN-based

An Acquirer of Maestro POS Transactions, ATM Transactions, and/or Manual Cash Disbursement Transactions occurring at PIN-based In-Branch Terminals may default route to the Network any such Transaction not belonging to its proprietary network. The Network determines whether or not the Transaction is being performed by a Cardholder.

The Acquirer must ensure that the files are loaded and functioning on its host systems and available to its Merchants, ATM Terminals, and PIN-based In-Branch Terminals for use within six calendar days from the date that each updated file is distributed. Upon receipt of an updated file, the Acquirer must confirm to Mastercard Switching Services via an acknowledgment file that it has updated its host systems accordingly.

5.4 Authorization and Clearing Requirements

This topic describes the authorization and clearing requirements.

5.4.1 Issuer Authorization Requirements

In the event that an Issuer chooses not to offer a particular Transaction message type to its Cardholders, the Issuer must provide a value of 57 indicating "transaction not permitted to issuer/cardholder" in DE 39 (Response Code) of the online authorization message.

5.4.2 Stand-In Processing Service

This Rule does not apply to an Issuer in the Europe Region if on or before 17 September 2008, the Issuer commenced its use of an alternative on-behalf authorization service that meets Mastercard Switching Services' performance standards as set forth in section 5.4.1.2 Performance Standards—Issuers of these Rules.

An Issuer is liable for all Transactions authorized (with or without PIN validation) using the Stand-In Processing Service, provided that the Network correctly uses the Stand-In Parameters defined by Mastercard Switching Services or the Issuer. The Issuer may establish Stand-In Processing Service PIN validation at its option.

For all of its Mastercard Card Programs, an Issuer must use the Stand-In Processing Service. Stand-In Investigation Service is now obsolete and replaced with Stand-In User Interface located in the Fraud Center. Stand-In Parameters for Mastercard (including Debit Mastercard) Card Programs must be set at or above Mastercard Switching Services' default limits.

In the event that fraudulent activity is detected with respect to a Mastercard BIN or BIN range, Mastercard Switching Services, in its sole discretion and judgment, may take such action as it deems necessary or appropriate to safeguard its goodwill and reputation.

Such action may include, by way of example and not limitation, declining some or all Transaction authorization requests received by the Stand-in Processing Service relating to the use of Cards issued under such BIN or BIN range.

For all of its Maestro and Cirrus Card Programs, an Issuer must use the Stand-In Processing Service. This requirement does not apply if the Issuer commenced its use of an alternative on-behalf authorization service before 1 December 2003 and such service meets Mastercard Switching Services' performance standards as set forth in section 5.4.2.2 Performance Standards—Issuers of these Rules.

Stand-In Parameters for Maestro and Cirrus Card Programs must be set at or above Mastercard Switching Services' default limits. An Issuer may employ a blocking service that declines all Transaction authorization requests during Stand- In processing for inactive BINs or in situations where Stand-In processing does not apply for regulatory reasons.

5.4.2.1 Accumulative Transaction Limits

An Issuer at its option, may use daily Stand-In Processing Service Transaction limits ("accumulative limits") for a Card Program that are higher than the applicable default limits set by Mastercard Switching Services.

Refer to the Stand-In Processing Forms 041a (Brand Product Categories Addendum), 041f (Accumulative Global Parameters), and 041g (Transaction Category Code Global Parameters) for the minimum (default) daily accumulative Transaction processing limit applicable to a particular Card Program.

5.4.2.2 Performance Standards—Issuers

For all Transactions, an Issuer authorization failure rate that exceeds one percent for two months in any six-month period is deemed to be substandard performance.

The Issuer failure rate is not applied until after the Issuer's fourth calendar month of operation or upon the Issuer's processing of 5,000 Transactions in a calendar month, whichever occurs first. The Issuer failure rate is calculated by taking the sum of ISO 8583 response codes 31—issuer signed off, 82—time out at Issuer host, and 96—system malfunction, and dividing by the total number of Transactions processed through the Issuer connection to the Network.

5.4.3 Authorization Responses

An Acquirer must comply with the authorization response wait time requirements set forth in Chapter 4 of the *Authorization Manual*.

An Issuer must comply with the authorization response requirements set forth in "Routing Timer Values" in Chapter 5 of the *Authorization Manual*. If the Issuer's response is not received within the required time frame, then the Transaction will time out and be forwarded via the Stand-In Processing System or another alternate authorization provider as specified by the Issuer.

5.4.4 Preauthorizations

An authorization request is properly identified as a preauthorization when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains a value of 4.

5.4.5 Final Authorizations

An authorization request is properly identified as a final authorization when DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status) contains a value of 0 and DE 48 (Additional Data), subelement 61 (POS Data Extended Condition Codes), subfield 5 contains a value of 1. An Acquirer in the Europe Region (excluding Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russian Federation, Tajikistan, Turkey, Turkmenistan, Uzbekistan, and Ukraine) that does not reverse an approved final authorization or does not clear an approved final authorization within three calendar days of the authorization date or clear for a different currency or transaction amount than what was authorized will be considered non-compliant with the final authorization performance standards.

5.4.6 Multiple Authorizations

The Acquirer must use a unique identifier from the initial approved authorization of a Transaction in any additional authorizations requested in connection with the same Transaction, by populating DE 48, subelement 63 (Trace ID) of each additional authorization request with the DE 63 (Network Data), subfield 1 (Financial Network Code) and subfield 2 (Banknet Reference Number) and DE 15 (Date, Settlement) data from the initial approved Authorization Request Response/0110 message. This unique identifier must also be included in the Transaction clearing record.

5.4.7 Full and Partial Reversals

An Acquirer must support reversals for the full amount of any authorized POS Transaction whenever the Acquirer host system is unable to communicate the authorization response to the POS Terminal.

5.4.8 Balance Inquiries

Balance inquiries are identified with a value of 30 in DE 3, subfield 1 of authorization messages.

5.4.9 CVC 2 Verification for POS Transactions

An Issuer must not authorize a Mastercard POS Transaction identified as a mail order, phone order, or e-commerce Transaction if the CVC 2 transmitted by the Acquirer does not match the CVC 2 on file with the Issuer corresponding to the Mastercard Account in question (that is, DE 48, subelement 87 of the Authorization Request Responses/0110 message = "N").

5.4.10 Decline Reason Code Service

For all Card-not-present Transactions, excluding mail order and telephone order (MO/TO) Transactions, the Decline Reason Code Service is an authorization functionality that translates specific Issuer-provided decline-related response code values to one of three Mastercard-provided values representing decline reason categories: Lifecycle, Policy, or Security.

A Merchant Advice Code (MAC) is also supplied for Card-not-present Transactions as applicable. In cases of recurring payment or Credential-on-file Transactions, for certain decline response

code values such as Expired Card, the service calls the Automatic Billing Updater (ABU) service to determine if a new expiry date is available. When a new expiry date is available, DE 48, subelement 84 (Merchant Advice Code) is appended into the response message with a value indicating to try again using the updated information; otherwise, an indicator to not try again is included. In the case of a security violation decline response code for Card-not-present Transactions, the Decision Intelligence service is called and based on the risk assessment, an appropriate fraud/security-related MAC value is determined and sent to the acquirer.

The Decline Reason Code Service intakes the decline reason from the Issuer, categorizes when appropriate, interprets the situation based on authorization data elements and additional Mastercard services, and prescribes to the Acquirer and Merchant the best course of action to take related to the decline through the decline reason and Merchant Advice codes. Technical and credit-related declines are not categorized as part of this service.

Issuer use of the DE 39 (Response Code) value of 05 (Do Not Honor) should not exceed 5% of all Mastercard and Maestro Card-not-present Transaction decline responses.

Authorization Request Response/0110 Response Codes

Value	Description	Action
79	Lifecycle (Mastercard use only)	Decline
82	Policy (Mastercard use only)	Decline
83	Security (Mastercard use only)	Decline

NOTE: Issuers must not utilize codes 79, 82, or 83 as these codes are reserved for Mastercard use only.

Specifically, as part of the Decline Reason Code Service (for more information refer to the Authorization Manual), these are the actions Merchants should take using the combination of - DE 48, subelement 84, and DE 39 to make better decisions on Card-not-present authorizations.

DE 39	DE 48, subelement 84	Merchant Advice Description	Merchant Action
79 or 82	01	Updated information needed	Updated information found to be available in Mastercard ABU database – secure new information before reattempting
79 or 82	03	Do not try again	Updated credentials were not found to be available in Mastercard ABU database – do not retry
83	01	Additional information needed	Ensure card information is correct. Authentication may improve likelihood of an approval – retry using authentication (such as EMV 3DS)

DE 39	DE 48, subelement 84	Merchant Advice Description	Merchant Action
83	03	Do not try again	Suspected Fraud – do not retry
79 or 82 or 83	02	Try again later	Retry transaction later

5.4.11 Account Status Inquiry (ASI) Requests

An ASI request is an Authorization Request/0100 message initiated by an Acquirer or Merchant to obtain the Issuer's validation that a Cardholder's Account is open and active.

An ASI request is identified with a value of 8 (Account Status Inquiry Service [ASI]) in DE 61 (Point-of-Service [POS] Data), subfield 7 (POS Transaction Status), and when submitted in connection with a purchase, contains a value of 00 (Purchase) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code). A Purchase ASI request must have a Transaction amount of zero.

Unless specifically permitted in the Standards, a purchase Transaction authorization request must not contain a Transaction amount value of one major unit of currency or any other nominal test amount that does not represent an actual purchase.

An Issuer that receives an ASI request must provide a valid and accurate value in DE 39 (Response Code) of the Authorization Request Response/0110 or Financial Transaction Request Response/0210 message. If a Mastercard or Debit Mastercard Account is open and active, the Issuer must provide a value of 00 (Approved) or 85 (Not Declined) in DE 39.

Mastercard will deem an Issuer to be noncompliant with this requirement if the Issuer declines an ASI request involving a Mastercard or Debit Mastercard Account and within 24 hours of such decline, approves a Transaction authorization request for a non-zero Transaction amount involving the same Merchant or Sponsored Merchant and the same Account. A noncompliant Issuer may be subject to fees under the global ASI Transaction Processing Excellence program.

5.4.12 Multiple Clearing Messages

A Mastercard Dual Message System Acquirer has the option of linking multiple presentments with partial amounts to one approved authorization identified as either a preauthorization or final authorization. The following requirements apply to Mastercard and Debit Mastercard Transactions acquired in the Mastercard Dual Message System:

1. In the First Presentment/1240 message, the Acquirer may must populate DE 25 (Message Reason Code) with either of the following values:
   a. **1403** (Previously approved authorization—partial amount, multi-clearing); or
   b. **1404** (Previously approved authorization—partial amount, final clearing). This value indicates that the original authorization is closed; no subsequent clearing messages may be submitted.

If the final first presentment message submitted for a preauthorized Transaction contains a value of 1403 in DE 25, and the total authorized amount has not been fully cleared, then the Acquirer or Merchant must initiate an authorization reversal so that the Issuer may release any excess hold on funds in the Cardholder's Account.

2. Upon receipt of a clearing message containing a value of 1403 or 1404, the Issuer must match the clearing message to the authorization message by comparing the data contained in the following fields:
   a. DE 63 (Transaction Life Cycle ID), subfield 2 (Trace ID) of the First Presentment/1240 message; and
   b. DE 63 (Network Data), subfield 2 (Banknet Reference Number) and DE 15 (Date, Settlement) of the Authorization Request/0100 message.

   NOTE: A Debit Mastercard Issuer may receive the value of 1403 or 1404 in DE 60 (Advice Reason Code), subfield 2 (Advice Reason Detail Code) of a Mastercard Single Message System-generated Financial Transaction Advice/0220 message.

3. Upon matching a clearing message to an authorization message, the Issuer must adjust any hold on the availability of funds in the Cardholder's Account in accordance with its standard Account management practice for cleared amounts:
   a. If the clearing message contains a value of **1403**, then the Issuer is advised to release the hold placed on the Cardholder's Account in connection with the approved authorization by the amount in DE 6 (Amount, Cardholder Billing); and
   b. If the clearing message contains a value of **1404**, then the Issuer is advised to release any unused funds in connection with the approved authorization.

5.5 Acceptance Procedures

5.5.1 Suspicious Cards

To report a suspicious Card to its Acquirer, the Merchant may include a value of 1 (Suspected fraud (merchant suspicious—code 10) in DE 61, subfield 8 (Transaction Security) of the authorization request message.

5.5.2 Obtaining an Authorization for a Mastercard POS Transaction

5.5.2.1 Authorization of Lodging, Cruise Line, and Vehicle Rental Transactions

If...	Then...
The authorization request message contains the Partial Approval Terminal Support Indicator, and the authorization request response message contains a value of 10 (Partial Approval) in DE 39 and a partial approval amount in DE 6.	The Transaction amount may not exceed the approved amount.

5.5.2.2 Authorization When the Cardholder Adds a Gratuity

If...	Then...
The authorization request message contains the Partial Approval Terminal Support Indicator, and the authorization request response message contains a value of 10 (Partial Approval) in DE 39 and a partial approval amount in DE 6.	The Transaction amount may not exceed the approved amount.

5.5.2.3 Use of Card Validation Code 2 (CVC 2)

All non-face-to-face gambling Transactions (MCC 7995) conducted with a Mastercard Card must include CVC 2 value in DE 48 (Additional Data—Private Use), subelement 92 of the Authorization Request/0100 message.

5.5.3 POS and Mastercard Manual Cash Disbursement Receipt Requirements

The "doing business as" (DBA) Merchant name, city, state/province, and country, or the financial institution location as provided in DE 43 (Acceptor Name/Location) must be included on a Transaction receipt.

5.5.4 POI Currency Conversion

The currency chosen by the Cardholder must be indicated as the Transaction currency in DE 49 of Transaction messages.

The POI currency conversion indicator and pre-conversion currency and amount must be provided in DE 54 of First Presentment/1240 messages.

5.6 Card-Present Transactions

This topic describes specifications relating to Card-present Transactions.

5.6.1 Chip Transactions at Hybrid POS Terminals

The Acquirer must send the EMV chip data in DE 55 (Integrated Circuit Card [ICC] System-Related Data) of the Authorization Request/0100 message and in DE 55 of the First Presentment/1240 message. A value of 2 or 6 must also be present in position 1 of the three-digit service code in DE 35 (Track 2 Data) of the Authorization Request/0100 message.

5.6.2 Offline Transactions Performed on Board Planes, Trains, and Ships

If applicable, the Acquirer must provide in the First Presentment/1240 message:

1. The value of F (Offline Chip) in DE 22 (Point of Service Entry Mode), subfield 7 (Card Data Input Mode).
2. The Application Authentication Cryptogram (AAC) in DE 55.

5.6.3 Contactless Transactions at POS Terminals

If a Maestro Card that also bears a domestic debit brand mark is used in a Contactless Transaction and the domestic debit brand does not support contactless payment functionality, the Transaction must be identified in all Transaction messages as a Maestro Contactless Transaction and all Rules regarding such Transactions apply to the Transaction.

If processed by means of the Network, the Maestro Contactless Transaction is identified by the following data elements:

1. In authorization:
   a. DE 22 (POS entry mode), subfield 1 (POS Terminal PAN Entry Mode) must contain the value of "7" to indicate PAN auto-entry via contactless M/Chip, and
   b. DE 61 (POS Data), subfield 11 (POS Card Data Terminal Input Capability) must contain the value of "3" to indicate contactless M/Chip.
2. In clearing:
   a. DE 22 (POS entry mode), subfield 1 (Terminal Data: Card Data Input Capability) must contain the value of "M" to indicate PAN auto-entry via contactless M/Chip, and
   b. DE 22 (POS data), subfield 7 (Card Data: Input Mode) must contain the value of "M" to indicate PAN auto-entry via contactless M/Chip.

5.6.4 Mastercard Contactless Transit Aggregated Transactions

A Mastercard Contactless transit aggregated Transaction occurs when the transit Merchant's Acquirer generates a First Presentment/1240 message combining one or more contactless taps performed with one Mastercard Account at one transit Merchant. A "tap" means the Cardholder's tap of the Card or Contactless Payment Device on the contactless reader of the POS Terminal with each ride taken.

An Acquirer submitting an authorization request to start a Contactless transit aggregated Transaction, either deferred or in real-time, must confirm the Issuer's authorization response was approved, in order to submit the First Presentment/1240 message to clear the aggregated transit fare. As an exception to the foregoing Standard, the Acquirer may submit a First Presentment/1240 message to claim transit debt, up to a specified limit in the country for deferred authorizations that were declined and unrecoverable, pursuant to the transit First Ride Risk (FRR) framework.

In order for the transit Merchant to receive chargeback protection, all of the following must occur:

1. The Merchant must send a properly identified Authorization Request/0100 message (which can be for any amount).
2. The Issuer must approve the Transaction.
3. The combined amount of the taps must be equal to or less than the applicable chargeback protection amount.
4. The maximum time period from the first tap until the First Presentment/1240 message is generated must be 14 calendar days or less.

Upon the Cardholder's request, the Merchant must provide a list of the taps (the date and fare for each ride taken) that were combined into a First Presentment/ 1240 message.

5.6.5 Maestro Contactless Transit Aggregated Transactions

A Maestro Contactless transit aggregated Transaction occurs when the Acquirer generates an Authorization Request/0100 message for an estimated amount in connection with the use of one Maestro Account at one transit Merchant.

Maestro Contactless transit aggregated Transactions must be processed as follows.

1. The Merchant sends an Authorization Request/0100 message with a value of 06 in DE 48, subelement 64, subfield 1 (Transit Transaction Type Indicator) for an estimated amount not to exceed the applicable Contactless transit Transaction ceiling limit amount.
2. The Issuer must approve the Transaction.
3. The Cardholder may make subsequent taps for additional rides; these taps will not be sent to the Issuer for authorization. The combined amount of the taps must be equal to or less than the post-authorized aggregated Contactless Transaction ceiling limit amount.
4. When the limit is reached or within three calendar days, the Merchant totals the value of all taps and generates a Reversal Request/0400 or Authorization Advice/0120 message to reverse any unused funds.

Upon the Cardholder's request, the Merchant must provide a list of the taps (the date and fare for each ride taken) that were combined into a First Presentment/ 1240 message.

5.6.6 Purchase with Cash Back Transactions

The authorization and clearing messages of each purchase with cash back Transaction must comply with the following requirements:

1. The Transaction must be identified with a value of 09 (purchase with cash back) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type).
2. The purchase amount, cash back amount, and total Transaction amount must be in the same currency.
3. The total Transaction amount (inclusive of the purchase and cash back amounts) must be transmitted in DE 4 (Amount, Transaction).
4. The cash back amount must be transmitted in DE 54 (Amounts, Additional).

5.6.7 Automated Fuel Dispenser Transactions

An automated fuel dispenser Transaction is identified in Authorization Request/0100 and Authorization Advice/0120 messages with MCC 5542 (Automated Fuel Dispenser) and a CAT level indicator of CAT 1 or CAT 2 (for Card-present Transactions) or CAT 6 (for e-commerce Transactions).

Authorization Before Fueling

Each automated fuel dispenser Transaction for which authorization is requested prior to the dispensing of fuel is properly processed as follows:

1. The Acquirer's initial Authorization Request/0100 message to the Issuer must be identified as a preauthorization and reflect one of the following:
   a. A maximum fuel dispense amount as determined by the Merchant or Acquirer; or
   b. A specific amount selected by the Cardholder; or
2. If the preauthorization request contains the partial approval support indicator, and the Issuer provides a partial approval response, then the final Transaction amount must not exceed the partial approval amount provided in DE 6 (Amount, Cardholder Billing), unless the preauthorization request amount was USD 1.
3. After the fuel is dispensed, the Acquirer must send an advice (0120 or 0420) message containing the final Transaction amount to the Issuer. The advice message must be sent no later than 20 minutes after the original preauthorization request.
4. If fuel is not dispensed or the Cardholder otherwise cancels the Transaction then within 20 minutes, the Acquirer must send either an advice (0120) message for a zero amount or a reversal (0400) message.
5. Within 60 minutes of receiving the advice message, the Issuer must release any hold that the Issuer placed on the Cardholder's available funds or credit in excess of the Transaction amount specified in DE 4 (Amount, Transaction).
   If the Issuer displays pending automated fuel dispenser Transaction information in Cardholder-facing applications, the information must be based on the advice message Transaction amount.
6. The Acquirer must send a First Presentment/1240 message with the final Transaction amount in DE 4 (Amount, Transaction).

Authorization After Fueling

If the Merchant initiates authorization after the fueling is completed, then the Acquirer's authorization request must be identified as a final authorization as described in section 5.4.5.

5.6.8 Electric Vehicle Charging Transactions

A Transaction occurring at an unattended POS Terminal for the purchase of electric vehicle charging services is identified with MCC 5552 (Electric Vehicle Charging) and a CAT level indicator of CAT 1 or CAT 2 (for Card-present Transactions) or CAT 6 (for e-commerce Transactions). Alternatively, if the primary business of the Merchant is temporary parking services, then MCC 7523 (Automobile Parking Lots and Garages) may be used. The Transaction may be authorized either prior to or after the vehicle charging, as follows.

Authorization Before Charging

Each electric vehicle charging Transaction for which authorization is requested before vehicle charging begins is properly processed as follows:

1. The Merchant must inform the Cardholder of any estimated amount for which authorization will be requested (for example, on a screen display or sticker at the Terminal) and must obtain the Cardholder's consent to the amount before initiating the authorization request. The estimated amount may be the Terminal's maximum dispense amount or a specific amount requested by the Cardholder.

2. The Acquirer's initial Authorization request/0100 message to the Issuer must be identified as a preauthorization. If the preauthorization request contains the partial approval support indicator, and the Issuer provides a partial approval response, then the final Transaction amount must not exceed the partial approval amount provided in DE 6 (Amount, Cardholder Billing).
3. If the Transaction is finalized for an amount that:
   a. Exceeds the authorized amount, then the Acquirer must send an additional (incremental) authorization request for the unauthorized amount; or
   b. Is less than the authorized amount, then within 24 hours of finalization, the Acquirer must either send a partial reversal for the excess authorized amount, or submit the Transaction clearing record.
4. In the case of a Transaction cancelled by the Cardholder, then within 24 hours, the Acquirer must send a full reversal request.

Authorization After Charging

If the Merchant initiates authorization after the vehicle charging is completed, then the Acquirer's authorization request must be identified as a final authorization as described in section 5.4.5.

5.7 Card-Not-Present Transactions

This section describes specifications relating to Card-not-present Transactions.

5.7.1 Electronic Commerce Transactions

If an e-commerce Transaction purchase will be delivered in multiple shipments, then effective 14 October 2022, each Merchant-initiated Transaction (MIT) authorization request for a partial shipment amount occurring subsequent to the original Cardholder-initiated Transaction (CIT) must be identified with the MIT value of M205 (Partial Shipment) in DE 48, subelement 22 (Multi-purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator).

5.7.1.1 Use of Static AAV for Card-not-present Transactions

In Belgium, an Issuer of Maestro Cards must technically support Card-not-present Transactions that contain a value of 3 in DE 48 (Additional Data—Private Use), subelement 43 (Static AAV), position 1 of Authorization Request/0100 messages.

5.7.2 Credential-on-file Transactions

A Credential-on-file Transaction must contain the Credential-on-file indicator, which is a value of:

- 10 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 1 (POS Terminal PAN Entry) of Authorization Request/0100 messages; and
- 7 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 7 (Card Data Input Mode) of First Presentment/1240 messages.

5.7.3 Recurring Payment Transactions

Each recurring payment Transaction must contain a value of 4 (Standing order/ recurring transactions) in DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence) in the Authorization Request/0100 message.

The initial Cardholder-initiated Transaction in a recurring payment arrangement must contain one of the following in DE 48 (Additional Data—Private Use), subelement 22 (Multi-Purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator):

- C101 (Credential-on-file [ad hoc])
- C102 (Standing Order [variable amount/fixed frequency])
- C103 (Subscription [fixed amount/fixed frequency])

Each subsequent Merchant-initiated Transaction in a recurring payment arrangement must contain one of the following in DE 48, subelement 22, subfield 5:

- M101 (Unscheduled Credential-on-file)
- M102 (Standing Order [variable amount/fixed frequency])
- M103 (Subscription [fixed amount/fixed frequency])

For recurring payment Transactions relating to a bill invoiced to the Cardholder, it is recommended that in the First Presentment/1240 message, the Merchant name in DE 43 subfield 1 be followed by a space, the word "BILL" or the local language equivalent, a space, and the bill reference number.

5.7.4 Installment Billing

5.7.4.1 Issuer-financed Single-authorization Installment Billing

The Issuer must use the following decline response codes when appropriate, and the relevant description must be reflected on the screen of the POS Terminal or the web page for the declined Transaction.

DE 39 (Response Code)	Description	Reason
13	Invalid amount	Transaction amount less than minimum set for country (e.g., HUF 20,000 in Hungary)
57	Transaction not permitted to Cardholder	Invalid number of installments, issuer does not offer Installment Transactions at all, or not for this specific Cardholder

DE 39 (Response Code)	Description	Reason
58	Transaction not permitted to Merchant	Installment Transactions must not be initiated by this Merchant (see "Exclusions")

5.7.4.2 Acquirer-financed and Merchant-financed Single-authorization Installment Billing

Transaction Processing Procedures

The Authorization Request/0100 message of a Transaction to be billed in installments must contain the following information, and must not contain the recurring payment indicator:

- The appropriate installment billing indicator code in DE 48, subelement 95 (Promotion Code), and
- The installment plan type and the number of installments requested by the Cardholder at the time of purchase in DE 112 (Additional Data, National Use). The Authorization Request/0100 message must be submitted for the total value of the Transaction. The Acquirer must ensure that the Authorization Request Response/0100 message contains the same number of installments indicated in DE 112 of the Authorization Request/0100 message.

The Acquirer must ensure that each installment payment clearing record contains information identifying the original approved authorization, as follows:

- The values contained in DE 63 (Network Data) and DE 15 (Settlement Date) from the authorization request response message must be placed in DE 63, subfield 2 (Trace ID) of each clearing record, and
- The value contained in DE 38 (Approval Code) from the authorization request response message must be placed in DE 38 of each clearing record.

5.7.4.3 Multiple-authorization Installment Billing

Installment Payment Information

An installment payment Transaction is properly identified as described in the following tables.

Table 1: Authorization Request/0100 and Financial Transaction Request/0200 Messages

In This Data Field:	If submitted by a Merchant, each Transaction must contain:	If submitted by an Installment Provider, each Transaction must contain:
DE 43 (Acceptor Name and Address)	The Merchant's name and address	The full or abbreviated name of the Installment Provider in combination with the retailer name, separated by an asterisk (for example, Installment Provider*Retailer)

In This Data Field:	If submitted by a Merchant, each Transaction must contain:	If submitted by an Installment Provider, each Transaction must contain:
DE 18 (Acceptor Type)	The MCC that best describes the primary business of the Merchant, or the nature of the purchase	The MCC that best describes the primary business of the retailer, or the nature of the purchase
DE 48, subelement 32 (Mastercard-assigned ID)	Optional; if present, the Mastercard-assigned ID of the Merchant	The Mastercard-assigned ID of the Installment Provider
DE 48, subelement 77 (Transaction Type Identifier)	Not Required	P10 (Purchase Repayment)
DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 5 (Cardholder/Merchant Initiated Transaction Indicator)	C104 for the initial CIT and M104 for each subsequent MIT	C104 for the initial CIT and M104 for each subsequent MIT

The following First Presentment/1240 message fields must be populated with the same information as provided in the corresponding Authorization Request/0100 message field:

- DE 43 (Acceptor Name/Location)
- DE 26 (Acceptor Business Code [MCC])
- PDS 0176 (Mastercard-assigned ID)
- PDS 0043 (Transaction Type Identifier)

The credential-on-file indicator must be present in authorization and clearing messages for each installment payment Transaction subsequent to the initial payment; refer to Rule 5.7.2.

If space allows, a message describing the installment being paid may optionally be provided in authorization and clearing messages at the end of DE 43, subfield 1 (Acceptor Name); for example, "PYMT 2 of 4".

Customer Service Information

The Acquirer is recommended to provide the following information in PDS 0170 (Acceptor Inquiry Information) of each First Presentment/1240 message:

- A customer service phone number for the retailer in subfield 1 (Customer Service Phone Number);
- A customer service phone number for the Installment Provider in subfield 2 (Acceptor Phone Number); and
- The installment number and total number of installments in subfield 3 (Additional Contact Information) (for example, "PAYMENT 2 of 4").

5.7.5 Transit Transactions Performed for Debt Recovery

A transit Merchant may use the transit debt recovery Transaction to recover a Cardholder's debt resulting from one or more contactless taps for entry to the transit system, if the Issuer has declined the Contactless transit aggregated Transaction Authorization Request/0100 message. A transit debt recovery Transaction is properly identified with:

- A value of 07 (Debt Recovery) in DE 48, subelement 64 (Transit Program), subfield 1 (Transit Transaction Type Indicator) in Authorization Request/0100 message and in PDS 0210 (Transit Program), subfield 1 (Transit Transaction Type Indicator) of First Presentment/1240 messages; and
- An amount in DE 4 (Amount, Transaction) that does not exceed the applicable Mastercard Contactless transit aggregated Transaction CVM limit.

An Issuer of Maestro Cards that allows its Cardholders to perform Maestro Contactless transit aggregated Transactions must be able to accept and must make an individual authorization decision for each transit debt recovery Transaction identified as a Card-not-present Transaction (for example, as a PAN key-entered, e-commerce, or mail order or telephone order (MO/TO) Transaction).

5.7.5.1 Transit First Ride Risk Framework

A Transit First Ride Risk (FRR) claim Transaction may be submitted when:

1. The Issuer declined the Contactless transit aggregated Transaction or a subsequent transit debt recovery Transaction using a response code value categorized in Table 1 as "Unrecoverable." In such event, the FRR claim Transaction can be submitted immediately; or
2. The Merchant made at least nine transit debt recovery Transaction attempts for a period of 45 calendar days from the date of the original Contactless Transit aggregated Transaction decline, with the last attempt occurring on day 45, and the Issuer declined each attempt for a "Recoverable" or "Temporarily Recoverable" reason. The Merchant must make no more than one attempt per 24-hour period.

An FRR claim Transaction does not require authorization by the Issuer. The FRR claim Transaction is properly identified in the First Presentment/1240 message with:

- A value of 08 (First Ride Risk Claim) in PDS 0210 (Transit Program), subfield 1 (Transit Transaction Type Indicator) for Post Authorized Aggregation (PAA), Authorized Aggregated Split Clearing (AASC) or PAA-Maestro transit model only; and
- An amount in DE 4 (Amount, Transaction) that does not exceed the FRR limit applicable in the Merchant's country, as specified in Chapter 5 of the Quick Reference Booklet.

The Acquirer must not submit an FRR claim Transaction if the Issuer used a response code value categorized in Table 1 as "Not Claimable" when declining the original Contactless transit aggregated Transaction or a subsequent transit debt recovery Transaction.

Table 2: Authorization Request Response/0110 Message DE 39 (Response Code) Decline Value Categories

Recoverable	Unrecoverable	Temporarily Recoverable	Not Claimable
• 51 (Insufficient funds/over credit limit) • 55 (Invalid PIN) • 61 (Exceeds withdrawal amount limit) • 65 (Exceeds withdrawal count limit) • 71 (PIN not changed) • 75 (Allowable number of PIN tries exceeded) • 76 (Invalid/ nonexistent "To Account" specified) • 77 (Invalid/ nonexistent "From Account" specified) • 78 (Invalid/ Nonexistent account specified)	• 03 (Invalid merchant) • 04 (Capture card) • 12 (Invalid transaction) • 13 (Invalid amount) • 14 (Invalid card number) • 41 (Lost card) • 43 (Stolen card) • 58 (Transaction not permitted to acquirer/terminal) • 62 (Restricted card) • 63 (Security violation) • 88 (Cryptographic failure)	• 01 (Refer to card issuer) • 05 (Do not honor)[1] • 70 (Contact card issuer) • 86 (PIN validation not possible) • 87 (Purchase amount only; no cash back allowed) • 91 (Authorization system or issuer system inoperative)	• 15 (Invalid issuer) • 30 (Format error) • 54 (Expired card) • 57 (Transaction not permitted to issuer/ cardholder) • 92 (Unable to route transaction) • 94 (Duplicate transmission detected) • 96 (System error)

5.7.6 Use of Automatic Billing Updater

The Automatic Billing Updater (ABU) is used by a Network Participant to communicate changes to Account information to Merchants that participate in recurring payment Transactions. For information about ABU, refer to the *Mastercard Automatic Billing Updater Reference Guide*, available on the Technical Resource Center through Mastercard Connect®.

5.8 Payment Transactions

This topic describes specifications relating to Transactions identified with a value of 28 (Payment Transaction) in DE 3 (Processing Code), subfield 1 (Cardholder Transaction Type Code) of authorization and clearing messages.

[1] Unrecoverable if DE 48, subelement 84 (Merchant Advice Code) contains a value of 03 (Do not try again).

5.8.1 Gaming Payment Transactions

1. The Gaming Payment Transaction must be properly identified in authorization and clearing messages using MCC 7995, and a Payment Transaction program type value of C04.
2. Gaming Payment Transactions will not be authorized in Mastercard Stand-In, X-Code or Limit 1. Authorization is entirely under the control of the Issuer.

For more information, refer to the *Mastercard Gaming and Gambling Payments Program Standards*, available on **Mastercard Connect** > **Technical Resource Center**.

5.9 POS Terminal Requirements

This topic describes POS terminal requirements.

5.9.1 Hybrid POS Terminal Requirements

A Hybrid POS Terminal is identified in Transaction messages with the following values:

- A value of 3, 5, 8, or 9 in DE 61 (Point-of-Service Data), Subfield 11 (POS Card Data Terminal Input Capability Indicator) in the Authorization Request/0100 message, as described in the Customer Interface Specification manual; and
- Data Input Capability) of the First Presentment/1240 message, as described in the IPM Clearing Formats manual.

A PIN-capable Hybrid POS Terminal is indicated when in addition, DE 22, Subfield 2 (Terminal Data: Cardholder Authentication Capability), of the First Presentment/ 1240 message contains a value of 1.

5.9.2 Mobile POS (MPOS) Terminals

All authorization and clearing messages for Transactions occurring at an MPOS Terminal must contain the MPOS acceptance device indicator, as follows:

- A value of 9 in DE 61 (Point-of-Service Data), subfield 10 (Cardholder-Activated Terminal Level) of the Authorization Request/0100 or Financial Transaction Request/0200 message; and
- A value of CT9 in PDS 0023 (Terminal Type) of the First Presentment/1240 message.

Chip-only MPOS Terminals

A Chip-only MPOS Terminal must use the following values:

- A value of 9 in DE 61 (Point-of-Service Data), Subfield 11 (POS Card Data Terminal Input Capability Indicator) in the Authorization Request/0100 message; and
- A value of E in DE 22 (Point of Service Data Code), Subfield 1 (Terminal Data: Card Data Input Capability) of the First Presentment/1240 message.

Software-based Chip-only MPOS Terminals

A software-based Chip-only MPOS Terminal must additionally use the following values:

- In the Authorization Request/0100 message, a value of:
  - 2 (Terminal does not have PIN entry capability) or 3 (MPOS Software-based PIN Entry Capability) in DE 22 (Point of Service Data Code), Subfield 2 (POS Terminal PIN Entry Mode)
  - 0 (Dedicated MPOS Terminal with PCI compliant dongle [with or without keypad]) or 1 (Off the Shelf Mobile Device) in DE 48 (Additional Data—Private Use), subelement 21 (Acceptance Data), subfield 1 (MPOS Acceptance Device Type)
- In the First Presentment/1240 message, a value of:
  - 2 (Terminal does not have PIN entry capability) or 3 (MPOS Software-based PIN Entry Capability) in DE 22 (Point of Service Data Code), Subfield 2 (Terminal Data: Card Data Input Capability)
  - 0 (Dedicated MPOS Terminal with PCI compliant dongle [with or without keypad]) or 1 (Off the Shelf Mobile Device) in PDS 0018 (Acceptance Data), subfield 1 (MPOS Acceptance Device Type)

5.10 Transaction Identification Requirements

This topic describes transaction identification requirements.

5.10.1 Transaction Date

The Transaction date must appear in DE 12 (Date and Time, Local Transaction) as follows.

For the following transaction...	The transaction date is the date on which...
Face-to-Face	The products or services are exchanged.
Non–Face-to-Face	The products are shipped or services performed.
Vehicle Rental	The vehicle is returned, or, if applicable, the prepayment date.
Lodging	Checkout occurred, or if applicable, the prepayment date.
No-show	The Cardholder was expected to arrive at the lodging merchant and failed to appear.
Airline/Railway	The airline or railway ticket was issued.
Cruise Line	The transportation documents were issued.
On-board Cruise Line	The passenger disembarks.
Refund	The Merchant grants a credit or price adjustment.

For the following transaction...	The transaction date is the date on which...
All In-Flight Commerce Transactions except those involving mailed purchases	The flight departs from the originating city. The Transaction date for in-flight commerce mailed purchases is the shipment date unless otherwise disclosed to the Cardholder.
Mastercard Contactless Transit Aggregated	One or more contactless taps performed with one Mastercard Account and occurring at one transit Merchant are aggregated in a First Presentment/1240 message.
Maestro Contactless Transit Aggregated	An Authorization Request/0100) message is sent for an estimated or maximum amount in connection with the use of one Maestro Account at one transit Merchant.

5.10.2 Contactless Transactions

The Acquirer must identify each Contactless Transaction with the following values. A Transaction must not be identified as a Contactless Transaction if the Card information is contact chip-read, magnetic stripe-read, or key-entered.

In addition, a Transaction must not be identified as a Maestro Contactless Transaction if the Card information is contactless magnetic stripe-read.

Table 3: Contactless Transaction Values for Authorization Request/0100 Message

Data Element	Subfield	Value
22 (Point of Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	One of the following: • 07 (PAN auto-entry via contactless M/Chip) • 91 (PAN auto-entry via contactless magnetic stripe)
61 (Point-of-Service [POS] Data)	11 (POS Card Data Terminal Input Capabilities)	One of the following: • 3 (Contactless M/Chip) • 4 (Contactless Magnetic Stripe)

Table 4: Contactless Transaction Values for First Presentment/1240 Messages

Data Element	Subfield	Value
22 (Point of Service [POS] Entry Mode)	1 (Terminal Data: Card Data Capability)	One of the following: • A (Contactless Magnetic Stripe [Proximity Chip]) • M (Contactless EMV/Chip [Proximity Chip])
22 (Point-of-Service Data Code)	7 (Card Data: Input Mode)	One of the following: • A (PAN auto-entry via contactless magnetic stripe) • M (PAN auto-entry via contactless M/Chip)

5.10.2.1 Contactless Transit Aggregated Transactions

The Acquirer must identify each Contactless transit aggregated Transaction with the following values.

Table 5: Contactless Transit Aggregated Transaction Values for Authorization Request/0100 Messages

Data Element	Subfield	Value
18 (Merchant Type)		One of the following: • 4111 (Transportation-Suburban and Local Commuter Passenger, and Local Commuter Passenger, including Ferries) • 4131 (Bus Lines) • 4784 (Bridge and Road Fees, Tolls)
22 (Point-of- Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	Any of the values shown in "Contactless Transactions Values for Authorization Request/0100 Messages." **NOTE: Additionally, the value of 82 appears in Contactless debt repayment Transactions.**

Data Element	Subfield	Value
48 (Additional Data— Private Use)	1 (Transaction Category Code [TCC])	X (Airline and Other Transportation Services)
48 (Additional Data— Private Use), subelement 64 (Transit Program)	1 (Transit Transaction Type)	One of the following: • 03 (Post-authorized Aggregated) • 06 (Post-authorized Aggregated Maestro)
61 (Point-of-Service [POS] Data)	1 (POS Terminal Attendance)	1 (Unattended terminal)
	3 (POS Terminal Location)	0 (On premises of merchant facility)
	4 (POS Cardholder Presence)	0 (Cardholder present)
	5 (POS Card Presence)	0 (Card present)
	6 (POS Card Capture Capabilities)	0 (Terminal/Operator has no card capture capability)
	7 (POS Transaction Status)	One of the following: • 0 (Normal request) • 4 (Pre-authorized request)
	10 (Cardholder-Activated Terminal Level)	0 (Not a CAT transaction)
	11 (POS Card Data Terminal Input Capability)	One of the following: • 3 (Contactless M/Chip) • 4 (Contactless Magnetic Stripe)

Table 6: Contactless Transit Aggregated Transaction Values for First Presentment/1240 Messages

Data Element	Subfield	Value
22 (Point of Service Data Code)	1 (Terminal Data: Card Data Capability)	One of the following: • A (PAN auto-entry via contactless magnetic stripe) • M (PAN auto-entry via contactless M/Chip)
	3 (Terminal Data: Card Capture Capability)	0 (No capture capability)
	4 (Terminal Operating Environment)	2 (On merchant premises; unattended terminal)

Data Element	Subfield	Value
	5 (Card Present Data)	0 (Cardholder present)
	6 (Card Present Data)	1 (Card present)
	7 (Card Data: Input Mode)	One of the following: • A (PAN auto-entry via contactless magnetic stripe) • M (PAN auto-entry via contactless M/Chip)
26 (Acceptor Business Code [MCC])		One of the following: • 4111 (Transportation-Suburban and Local Commuter) Passenger, including Ferries) • 4131 (Bus Lines) • 4784 (Bridge and Road Fees, Tolls)
PDS 0210 (Transit Transaction Type)	1 (Transit Transaction Type)	One of the following: • 03 (Post-authorized Aggregated) • 06 (Post-authorized Aggregated Maestro)

5.10.2.2 Contactless-only Transactions

The Acquirer must identify each Contactless-only Transaction with the following values.

Table 7: Contactless-Only Transaction Values for Authorization Request/0100

Data Element	Subfield	Value
18 (Merchant Type)		An MCC approved to be contactless-only as published by Mastercard from time to time in the *Global Operations Bulletin*.
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	Any of the values shown in "Contactless Transactions Values for Authorization Request/0100 Messages."
61 (Point-of-Service [POS]) Data	1 (POS Terminal Attendance)	1 (Unattended terminal)

Data Element	Subfield	Value
	3 (POS Terminal Location)	One of the following: • 0 (On premises of merchant facility) • (Off premises of merchant facility [merchant terminal—remote location])
	4 (POS Cardholder Presence)	0 (Cardholder present)
	5 (POS Card Presence)	0 (Card present)
	7 (POS Transaction Status)	0 (Normal request)
	10 (Cardholder-Activated Terminal Level)	One of the following: • 1 (Authorized Level 1 CAT: Automated dispensing machine with PIN) • 2 (Authorized Level 2 CAT: Self-service terminal) • 3 (Authorized Level 3 CAT: Limited amount terminal)
	11 (POS Card Data Terminal Input Capability)	One of the following: • 3 (Contactless M/Chip) • 4 (Contactless Magnetic Stripe)

Table 8: Contactless-Only Transaction Values for First Presentment/1240

Data Element	Subfield	Value
22 (Point of Service Data Code)	1 (Terminal Data: Card Data Capability)	One of the following: • A (PAN auto-entry via contactless magnetic stripe) • M (PAN auto-entry via contactless M/Chip)
	4 (Terminal Operating Environment)	One of the following: • 2 (On merchant premises; unattended terminal) • 4 (Off merchant premises; unattended) • 6 (Off cardholder premises; unattended)

Data Element	Subfield	Value
	5 (Card Present Data)	0 (Cardholder present)
	6 (Card Present Data)	1 (Card present)
	7 (Card Data: Input Mode)	One of the following: • A (PAN auto-entry via contactless magnetic stripe) • M (PAN auto-entry via contactless M/Chip)
26 (Acceptor Business Code [MCC])		An MCC approved to be contactless-only as published by Mastercard from time to time in the *Global Operations Bulletin*.

5.10.3 Payment Transactions

The Acquirer must identify each Payment Transaction, MoneySend Payment Transaction, and Gaming Payment Transaction, as applicable, with the following values.

Table 9: Payment Transaction Values for Authorization Request/0100 Messages

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	28

Data Element	Subfield	Value
18 (Acceptor Type)		One of the following: • 6532—for a Payment Transaction processed by a Network Participant or its authorized agent. • 6533—for a Payment Transaction processed by a Merchant. • 6536—for Intracountry MoneySend Payment Transactions • 6537—for Intercountry MoneySend Payment Transactions • 7994—for Gaming Payment Transactions (Video Game Arcades/Establishments) • 7995—for Gaming Payment Transactions (gambling Transactions) • A value specified for Payment Transactions in the applicable intracountry or intercountry business service arrangement, if one is in place
48 (Additional Data: Private Use)	TCC (Transaction Category Code)	P
48 (Additional Data: Private Use)	77 (Transaction Type Identifier)	Payment Transaction program type

Table 10: Payment Transaction Values for First Presentment/1240 Messages

Data Element	Subfield	Value
3 (Processing Code)	1 (Cardholder Transaction Type)	28
26 (Acceptor Business Code)		As described for DE 18 (Acceptor Type) in the Authorization Request/ 0100 message
48 (Additional Data: Private Use)	PDS 0043 (Transaction Type Identifier)	Payment Transaction program type

The value used for the Payment Transaction program type must be that which best describes the purpose of the Payment Transaction.

The Acquirer also should provide either the Network Participant service phone number in PDS 0170 (Acceptor Inquiry Information), subfield 1 (Network Participant Service Phone Number) or the URL address in PDS 0175 (Acceptor URL) in the clearing message.

A Payment Transaction Detail addendum may also be submitted with a Payment Transaction. This addendum provides the Issuer and Cardholder with enhanced data about the Merchant, the recipient of funds, and other Transaction details.

5.10.4 Electronic Commerce Transactions

The Acquirer must identify each electronic commerce Transaction with the following values.

Table 11: Electronic Commerce Transaction Values for Authorization Request/0100 Messages

Data Element	Subfield	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	One of the following: • 09 (PAN/Token entry via electronic commerce containing DSRP cryptogram in DE 55 (Integrated Circuit Card [ICC] System-Related Data)) • 10 (Credential on File) • 81 (PAN/Token entry via electronic commerce with optional Identity Check AAV or DSRP cryptogram in UCAF)
61 (Point-of-Service [POS] Data)	4 (POS Cardholder Presence)	One of the following: • 4 (Standing order/recurring transactions [If the Transaction is the first payment in a recurring payment arrangement]) • 5 (Electronic order)
61 (Point-of-Service [POS] Data)	10 (CAT Level)	6 (Electronic commerce)

Table 12: For First Presentment/1240 Messages

Data Element	Subfield	Value
22 (Point of Service Data Code)	5 (Cardholder Present Data)	One of the following: • 4 (Cardholder not present (standing order/recurring transactions [If the Transaction is the first payment in a recurring payment arrangement]) • 5 (Cardholder not present [electronic order])
22 (Point of Service Data Code)	7 (Card Data: Input Mode)	7 (Credential-on-file) or S (Electronic commerce)

5.10.5 Digital Secure Remote Payment Transactions

A Digital Secure Remote Payment Transaction is an electronic commerce Transaction that contains cryptographic information, in the form of either full EMV chip data passed in DE 55 or a cryptographic value derived from an M/Chip cryptogram passed in the Digital Payment Data field. Subsequent to the initial Digital Secure Remote Payment Transaction, a related Transaction for a partial shipment may occur, in which case cryptographic information is not passed.

When a Digital Secure Remote Payment Transaction contains tokenized account information, the Mastercard Digital Enablement Service performs token mapping and cryptographic validation services.

5.10.5.1 Digital Secure Remote Payment Transactions Containing Chip Data

Table 13: Authorization Request/0100 Messages

Data Element	Subfield/Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode	09 (PAN entry via electronic commerce including remote chip)
48 (Additional Data— Private Use)	33 (PAN Mapping File Information)	Present when the Mastercard Digital Enablement Service performs token mapping.

Data Element	Subfield/Subelement	Value
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs token mapping: • Subfield 1 = 50 (Mastercard Digital Enablement Service PAN Mapping); and • Subfield 2 = C (Conversion of Device Account Number to Funding Account Number was completed)
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs cryptographic validation: • Subfield 1 = 51 (Mastercard Digital Enablement Service Chip Pre-Validation); and • Subfield 2 = V (Valid)
61 (Point-of-Service [POS] Data)	3 (POS Terminal Location)	One of the following: • 2 (Off premises of acceptor facility [cardholder terminal including home PC, mobile phone, PDA]); or • 4 (On premises of acceptor facility [cardholder terminal including home PC, mobile phone, PDA])
	4 (POS Cardholder Presence)	5 (Electronic order [home PC, Internet, mobile phone, PDA])
	10 (Cardholder-Activated Terminal Level)	6 (Authorized Level 6 CAT: Electronic commerce Terminal Level)

Table 14: First Presentment/1240 Messages

Data Element	Subfield/PDS	Value
22 (Point-of- Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: • 2 (On acceptor premises; unattended terminal); or • 4 (Off acceptor premises; unattended)

Data Element	Subfield/PDS	Value
	5 (Cardholder Present Data)	5 (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	R (PAN Entry via electronic commerce, including remote chip)
48 (Additional Data)	PDS 0023 (Terminal Type)	CT 6 (CAT level 6 [electronic commerce transaction])

5.10.5.2 Digital Secure Remote Payment Transactions Containing Digital Payment Data

Table 15: Authorization Request/0100 Messages

Data Element	Subfield/Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	One of the following: • 10 (Credential-on-file) • 81 (PAN/Token entry via electronic commerce with optional Identity Check AAV or DSRP cryptogram in UCAF)
48 (Additional Data—Private Use)	33 (PAN Mapping File Information)	Present when the Mastercard Digital Enablement Service performs token mapping.
	42 (Electronic Commerce Indicators), subfield 1, position 3 (UCAF Collection Indicator)	All of the following (UCAF authentication occurs): • Position 1 = 2 • Position 2 = 4 • Position 3 = 2 or 6
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs token mapping: • Subfield 1 = 50 (Mastercard Digital Enablement Service PAN Mapping); and • Subfield 2 = C (Conversion of Device Account Number to Funding Account Number was completed)

Data Element	Subfield/Subelement	Value
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs cryptographic validation: • Subfield 1 = 51 (Mastercard Digital Enablement Service Chip Pre-Validation); and • Subfield 2 = V (Valid)
61 (Point-of-Service [POS] Data		
DE 104 (Digital Payment Data)	001 (Digital Payment Cryptogram)	001 (Digital Payment Cryptogram

Table 16: First Presentment/1240 Messages

Data Element	Subfield/PDS	Value
22 (Point-of- Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: • 2 (On acceptor premises; unattended terminal); or • 4 (Off acceptor premises; unattended)
	5 (Cardholder Present Data)	5 (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data: Input Mode)	S (Electronic commerce)
48 (Additional Data)	PDS 0023 (Terminal Type)	CT 6 (CAT level 6 [electronic commerce transaction])
	PDS 0052 (Electronic Commerce Security Level Indicator)	All of the following (UCAF authentication occurs): • Position 1 = 2 • Position 2 = 4 • Position 3 = 2 or 6

5.10.5.3 Merchant-initiated Transactions following Digital Secure Remote Payment Transactions

Table 17: Authorization Request/0100 Messages

Data Element	Subfield/Subelement	Value
22 (Point-of-Service [POS] Entry Mode)	1 (POS Terminal PAN Entry Mode)	81 (PAN entry via electronic commerce, including chip)
48 (Additional Data—Private Use)	33 (PAN Mapping File Information)	Present when the Mastercard Digital Enablement Service performs token mapping.
	42 (Electronic Commerce Indicators), subfield 1, position 3 (UCAF Collection Indicator)	All of the following (UCAF authentication occurs): • Position 1 = 2 • Position 2 = 4 • Position 3 = 7
	71 (On-behalf Services)	Present when the Mastercard Digital Enablement Service performs token mapping: • Subfield 1 = 50 (Mastercard Digital Enablement Service PAN Mapping); and • Subfield 2 = C (Conversion of Device Account Number to Funding Account Number was completed) **NOTE: Value 51 (Mastercard Digital Enablement Service Chip Pre-Validation) does not appear in a partial shipment.**

Table 18: First Presentment/1240 Messages

Data Element	Subfield/PDS	Value
22 (Point-of- Service [POS] Data Code)	4 (Terminal Operating Environment)	One of the following: • 2 (On acceptor premises; unattended terminal); or • 4 (Off acceptor premises; unattended)

Data Element	Subfield/PDS	Value
	5 (Cardholder Present Data)	5 (Cardholder not present [electronic order (PC, Internet, mobile phone, or PDA)])
	7 (Card Data : Input Mode)	S (Electronic commerce)
48 (Additional Data)	PDS 0023 (Terminal Type)	CT 6 (CAT level 6 [electronic commerce transaction])
	PDS 0052 (Electronic Commerce Security Level Indicator)	All of the following (no UCAF authentication occurs): • Position 1 = 2 • Position 2 = 4 • Position 3 = 7

5.10.6 Cardholder-initiated Transactions

The Acquirer must identify each Cardholder-initiated Transaction (CIT) that is also a Credential-on-file Transaction in Authorization Request/0100 messages with one of the following values as applicable, in addition to populating all other required data. These values may optionally be used in CITs occurring in other acceptance environments. When populated in an Authorization Request/0100 message, the same value may also be provided in the First Presentment/1240 message.

Table 19: CIT values for Authorization Request/0100 Messages

Data Element/ Subelement	Value	Use this value when...	Examples
DE 48, subelement 22 (Multi-purpose Merchant Indicator), subfield 5 (Cardholder/ Merchant Initiated Transaction Indicator)	C101 (Credential-on-file [ad hoc])	The Cardholder is authorizing the Merchant to store the Cardholder's Account data for subsequent use in connection with one or more later Transaction(s) with that Merchant (a "COF arrangement").	The Cardholder initiates a purchase and agrees that the Merchant may store the credential for future purchases.

Data Element/ Subelement	Value	Use this value when...	Examples
	C102 (Standing Order [variable amount/fixed frequency])	The Cardholder is agreeing to a COF arrangement with the Merchant for a series of recurring payments of **variable amount and fixed frequency** and is initiating the first payment.	The Cardholder initiates the first in a series of monthly utility payments, where the amounts will vary based on electricity consumption.
	C103 (Subscription [fixed amount/fixed frequency])	The Cardholder is agreeing to a COF arrangement with the Merchant for a series of recurring payments of **fixed amount and fixed frequency** and is initiating the first payment. The subscription arrangement may include an allowance for price changes to occur from time to time.	The Cardholder initiates the first in a series of quarterly newspaper subscription payments of fixed amounts.
	C104 (Installment)	The Cardholder has expressly authorized a COF arrangement with the Merchant for an installment billing plan and is initiating the first payment. The installment billing must be for a **single purchase** of goods or services with a known amount and set frequency over a specified duration.	The Cardholder agrees to enter into an installment billing plan for the purchase of a television and to make the first payment.

Table 20: CIT Values for First Presentment/1240 Messages

Data Element/PDS	Value
PDS 0218 (Cardholder/Merchant Initiated Transaction Indicator)	One of the following: • C101 (Credential-on-file [ad hoc]) • C102 (Standing Order [variable amount/fixed frequency]) • C103 (Subscription [fixed amount/fixed frequency]) • C104 (Installment)

5.10.7 Merchant-initiated Transactions

The Acquirer must identify each Merchant-initiated Transaction (MIT) in Authorization Request/0100 messages with one of the following values as applicable, in addition to populating all other required data. The value of M1XX means "Merchant-initiated recurring payment or installment" and the value of M2XX means "Merchant-initiated industry practice". When populated in an Authorization Request/0100 message, the same value may also be provided in the First Presentment/1240 message.

Table 21: MIT Values for Authorization Request/0100 Messages

Data Element/ Subelement	Value	Use this value when...	Examples
DE 48, subelement 22 (Multi-purpose Merchant Indicator), subfield 5 (Cardholder/ Merchant Initiated Transaction Indicator)	M101 (Unscheduled Credential-on-file)	The Cardholder has expressly authorized the Merchant to store the Cardholder's Account data for subsequent use in connection with one or more later Transaction(s) with that Merchant (a "COF arrangement").	The Merchant initiates a Transaction to "top-up" the Cardholder's tollway account based on a prearranged reload schedule.
	M102 (Standing Order [variable amount/fixed frequency])	The Cardholder has expressly authorized a COF arrangement with the Merchant for a series of recurring payments of **variable amount and fixed frequency**.	The Merchant initiates a Transaction for the Cardholder's next monthly utility payment.

Data Element/ Subelement	Value	Use this value when...	Examples
	M103 (Subscription [fixed amount/fixed frequency])	The Cardholder has expressly authorized a COF arrangement with the Merchant for a series of recurring payments of **fixed amount and fixed frequency**, which may include an allowance for price changes to occur from time to time.	The Merchant initiates a Transaction for the Cardholder's next quarterly newspaper subscription payment.
	M104 (Installment)	The Cardholder has expressly authorized a COF arrangement for an installment billing plan relating to a single purchase of goods or services with a known amount and set frequency over a specified duration.	The Merchant initiates a Transaction for the Cardholder's next biweekly installment payment for the purchase of a television.
	M205 (Partial Shipment)	One or more items in the Cardholder's purchase order was out of stock at the time that the Cardholder initiated payment. The Merchant initiates a separate Transaction for the remaining items when ready to be shipped.	The Cardholder originally ordered a hat and sunglasses, but the hat was out of stock. The Cardholder completes the purchase of the sunglasses and agrees to wait for the hat to be restocked. The Merchant initiates a partial shipment Transaction for the hat when back in stock.
	M206 (Related/Delayed Charge)	After completing a payment, the Cardholder owes an additional amount to the Merchant based on the original Transaction terms.	The Merchant initiates a related/delayed charge Transaction for mini-bar charges after the Cardholder has checked out of the hotel.

Data Element/ Subelement	Value	Use this value when...	Examples
	M207 (No-show	Under the Merchant's guaranteed reservation service policy, the Cardholder owes a no-show fee.	The Merchant initiates a Transaction to collect a no-show fee when the Cardholder does not cancel a guaranteed reservation within the previously disclosed cancellation time frame.
	M208 (Resubmission)	The Merchant's previous attempt to obtain authorization for a Transaction was declined but the Issuer's response does not prohibit the Merchant from trying again later.	• The Merchant initiates an authorization request after receiving a previous "insufficient funds/ over credit limit" response. • The Merchant initiates a transit debt recovery Transaction.

Refer to Table 4 for value usage information.

Table 22: MIT Values for First Presentment/1240 Message

Data Element/PDS	Value
PDS 0218 (Cardholder/Merchant Initiated Transaction Indicator)	One of the following: • M101 (Unscheduled Credential-on-file) • M102 (Standing Order [variable amount/fixed frequency]) • M103 (Subscription [fixed amount/fixed frequency]) • M104 (Installment) • M205 (Partial Shipment) • M206 (Related/Delayed Charge) • M207 (No-show) • M208 (Resubmission)

5.11 Cardholder-Activated Terminal (CAT) Transactions

In Authorization Request/0100 and Authorization Request Response/0110 messages, the CAT level indicator is located in DE 61 (Point-of-Service Data), subfield 10 (Cardholder-Activated Terminal Level). In First Presentment/1240, Chargeback/1442, Second Presentment/1240, and Arbitration Chargeback/1442 messages, the CAT level indicator is located in PDS 0023 (Terminal Type).

For additional requirements, see the *Customer Interface Specification* and the *IPM Clearing Formats* manuals.

The First Presentment/1240 message of a CAT Transaction must contain one of the following values in DE 22 (Point of Service Data Code), subfield 7 (Card Data: Input Mode):

- A (PAN auto-entry via contactless magnetic stripe)
- B (Magnetic stripe reader input, with track data captured and passed unaltered; does not apply to CAT 3)
- C (Online Chip)
- F (Offline Chip)
- M (PAN auto-entry via contactless M/Chip)
- N (Contactless input, Contactless Mapping Service applied [This value is visible only to Issuer; Acquirers use value A or M])
- S (Electronic commerce; applies to CAT 6 only)
- 2 (Magnetic stripe reader input; applies to CAT 3 only)

5.11.1 CAT Level Requirements

This topic describes CAT level requirements.

5.11.1.1 CAT Level 1: Automated Dispensing Machines (CAT 1)

The following authorization requirement applies to CAT 1 devices:

The MIP X-Code authorization response must be a decline. The Issuer is liable for Transactions that are approved under acquirer MIP X-Code, up to the MIP X-Code limits specified by Mastercard Switching Services.

5.11.1.2 CAT Level 2: Self-Service Terminal (CAT 2)

The following authorization requirement applies to CAT 2 devices:

The issuer is liable for Transactions that are approved under acquirer MIP X-Code, up to the MIP X-Code limits specified by Mastercard Switching Services.

5.11.1.3 CAT Level 3: Limited Amount Terminals (CAT 3)

The following authorization requirement applies to CAT 3 devices:

X-code processing does not apply.

5.11.1.4 CAT Level 4: In-Flight Commerce (IFC) Terminals (CAT 4)

The following authorization requirement applies to CAT 4 devices:

The Issuer is liable for Transactions that are approved under acquirer MIP X-Code, up to the MIP X-Code limits specified by Mastercard Switching Services.

5.11.1.5 CAT Level 9: Mobile POS (MPOS) Acceptance Device Transactions (CAT 9)

The Acquirer must submit the following values in Transaction messages for each Transaction conducted at an MPOS Terminal:

- A value of 9 (MPOS Acceptance Device) in DE 61 (Point-of-Service[POS] Data), subfield 10 (Cardholder-Activated Terminal Level) of the Authorization Request/ 0100 message; and
- A value of CT9 (MPOS Acceptance Device) in PDS 0023 (Terminal Type) of the First Presentment/1240 message.

Chapter 6 Private Label Requirements

See the Private Label Rules manual.

Private Label Requirements

Private Label Requirements

See the *Private Label Rules* manual for information regarding Private Label requirements.

Chapter 7 Other Schemes

Mastercard Switching Services does not currently provide switching services for other schemes.

Other Schemes

Other Schemes

Applicable rules will be added here as and when additional processing services are offered.

Appendix A Annexes to Rule 2.4 Confidential Information of Network Participants

This appendix provides additional information for Rule 2.4.

List of parties and description of transfer

A. List of Parties

1. Data exporter: Mastercard Switching Services
   - Name and Address of Mastercard Switching Services as well as the name, position, and contact details for the Mastercard Switching Services' contact person: as stipulated in the relevant enrollment form, announcement, license agreement or any other documents by which Network Participant is bound.
   - Activities relevant to the data transferred: Activity and Digital Activity.
   - Signature and date: as stipulated in the relevant enrollment form, announcement, license agreement or another documents by which Network Participant is bound.
   - Role: As set out in Clause **2.4.2 of those Standards** or as stipulated in the relevant enrollment form, announcement, license agreement or any other documents by which Network Participant is bound.
2. Data importer: Network Participant
   - Name and Address of Network Participant as well as the name, position, and contact details for Network Participant's contact person: as stipulated in the relevant enrollment form, announcement, license agreement or any other relevant documents by which Network Participant is bound.
   - Activities relevant to the data transferred: Participating in, or benefiting from, the Activity or Digital Activity.
   - Signature and date: as stipulated in the relevant enrollment form, announcement, or license agreement by which Network Participant is bound by those Standards.
   - Role: As set out in Clause 2.4.2 of those Standards or as stipulated in the relevant enrollment form, announcement, license agreement or any other documents by which Network Participant is bound.

B. Description of the Transfer

Data Subjects

As stipulated in the relevant enrollment form, announcement, license agreement or any other relevant documents by which Network Participant is bound.

Categories of data

Transaction data, including PAN data, date, time, and amount of transaction or as stipulated in the relevant enrollment form, announcement, license agreement or any other relevant documents by which Network Participant is bound.

Sensitive Data transferred

The Parties do not Process any Sensitive Data in the context of the Activity and the Digital Activity unless as stipulated otherwise in the relevant enrollment form, announcement, license agreement or any other relevant documents by which Network Participant is bound.

Frequency of the transfer

Continuous

Nature of the Processing

Collection, storage, analysis, disclosure by transfer or otherwise making available.

Purposes of the transfer(s)

The transfer is made for the purposes set forth in clause 2.4.2 of those Standards or as stipulated in the relevant enrollment form, announcement, license agreement or any other relevant documents by which Network Participant is bound.

Period for which the Personal Data will be retained

Personal Data will be retained only for as long as necessary to provide the services covered under the Activity and the Digital Activity.

Technical and organizational measures to ensure the security of data

The Customer and the Corporation will, as a minimum, implement the following types of security measures:

Physical access control

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

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

Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons, including:

- User identification and authentication procedures;
- ID/password security procedures (e.g., special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);

- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts; and
- Creation of one master record per user, user master data procedures, per data processing environment.

Data access control

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

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

Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, including:

- Tunneling;
- Logging; and
- Transport security.

Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including:

- Logging and reporting systems; and
- Audit trails and documentation.

Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the instructions of the Controller, including:

- Unambiguous wording for the Controller's instructions;
- Formal commissioning (request form); and
- Criteria for selecting the Processor.

Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical or logical), including:

- Backup procedures;
- Mirroring of hard disks (e.g., RAID technology);
- Uninterruptible power supply;
- Remote storage;
- Anti-virus/firewall systems; and
- Disaster recovery plan.

Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately, including:

- Separation of databases;
- Access and use restrictions on a need-to-know basis;
- Segregation of functions (e.g., production or testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

Sub-processing of personal data

List of Sub-Processors

As listed in *Mastercard Subprocessor Information* or in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Appendix B Compliance Zones

This section identifies the noncompliance category that the Network has assigned to the Standards described within this manual.

Compliance Zones

Compliance Zones

Rule Section and Title	Compliance Zone
1.1.5 Certification	C
1.2.3 Rights, Liabilities and Obligations of a Network Participant following Termination	A
1.3 Conduct of Network Activity	A
1.6 Examination and Audit	A
2.1 Integrity of the Network	A
2.2 Fees, Assessments and Other Payment Obligations	A
2.3 Obligation of Network Participant to Provide Information	C
2.4 Confidential Information of Network Participants	A
2.5 Cooperation	B
3.1 Net Settlement	A
4.1 Connecting to the Network	A
4.2 Routing Instructions and System Maintenance	C
5.1 Transaction Message Data	A
5.2 Authorization Routing – Mastercard POS Transactions	A
5.3 Authorization Routing – Maestro POS, ATM Terminal and PIN-based In-branch Terminal Transactions	A
5.4 Authorization and Clearing Requirements	A
5.5.1 Suspicious Cards	B
5.5.2 Obtaining an Authorization for a Mastercard POS Transaction	A
5.5.3 POS and Mastercard Manual Cash Disbursement Receipt Requirements	B
5.5.4 POI Currency Conversion	B
5.6.1 Chip Transactions at Hybrid POS Terminals	A
5.6.2 Offline Transactions Performed on Board Planes, Trains and Ships	B
5.6.3 Contactless Transactions at POS Terminals	A
5.6.4 Mastercard Contactless Transit Aggregated Transactions	A
5.6.5 Maestro Contactless Transit Aggregated Transactions	A
5.6.6 Purchase With Cash Back Transactions	A

Compliance Zones

Rule Section and Title	Compliance Zone
5.6.7 Automated Fuel Dispenser Transactions	A
5.7.1 Use of Static AAV for Card-not-present Transactions	A
5.7.2 Recurring Payment Transactions	A
5.7.3 Installment billing for Domestic Transactions – Participating Countries Only	A
5.7.4 Transit Transactions Performed for Debt Recovery	A
5.7.5 Use of Automatic Billing Updater	B
5.8.1 Gaming Payment Transactions	A
5.9.1 Hybrid POS Terminal Requirements	A
5.10 Transaction Identification Requirements	A
5.11 Cardholder-Activated Terminal (CAT) Transactions	A

Appendix C Definitions

This appendix contains defined terms used in this manual.

Definitions

The following terms as used in this manual have the meanings set forth below.

Additional and revised terms may also be used for purposes of the Rules in a particular chapter or section of this manual.

Access Device

A device other than a Card that has successfully completed all applicable Mastercard certification and testing requirements, if any, and:

- Uses at least one Payment Application provisioned to the device by or with the approval of a Customer to provide access to an Account; • Supports the transmission or exchange of data using one or both of the following
  - Magnetic stripe or chip data containing a dynamic cryptogram to or with a Terminal, as applicable, by implementing the EMV Contactless Specifications (Book D) to effect Transactions at the Terminal without requiring direct contact of the device to the Terminal
  - Chip data containing a dynamic cryptogram to or with a Terminal, as applicable, by implementing the Mastercard Cloud-Based Payments (MCBP) documentation to effect Transactions at the Terminal by capture of a QR Code containing the Transaction Data
- May also support the transmission of magnetic stripe data containing a dynamic cryptogram to a Terminal to effect Transactions identified by the Acquirer in Transaction messages as magnetic stripe Transactions.

A Cirrus Access Device, Maestro Access Device, and Mastercard Access Device is each an Access Device. Also see Mobile Payment Device.

Account

An account maintained by or on behalf of a Cardholder by an Issuer for the processing of Transactions, and which is identified with a bank identification number (BIN) or Issuer identification number (IIN) designated by the Corporation in its routing tables for routing to the Interchange System. Also see Cirrus Account, Maestro Account, Mastercard Account.

Acquirer

A Customer in its capacity as an acquirer of a Transaction.

ATM Terminal

An ATM that enables a Cardholder to effect an ATM Transaction with a Card (and if contactless-enabled, an Access Device) in accordance with the Standards.

ATM Transaction

A cash withdrawal effected at an ATM Terminal with a Card and processed through the Mastercard ATM Network. An ATM Transaction is identified with MCC 6011 (Automated Cash Disbursements—Customer Financial Institution).

Bank Branch Terminal

An attended device, located on the premises of a Customer or other financial institution designated as its authorized agent by the Corporation, that facilitates a Manual Cash Disbursement Transaction by a Cardholder.

Card

A card issued by a Customer pursuant to License and in accordance with the Standards and that provides access to an Account. Unless otherwise stated herein, Standards applicable to the use and acceptance of a Card are also applicable to an Access Device and, in a Card-not-present environment, an Account. A Cirrus Card, Maestro Card, and Mastercard Card is each a Card.

Card Program

A Card issuing program of an Issuer that is the Network Participant.

Cardholder

The authorized user of a Card or Access Device issued by a Customer.

Cardholder-initiated Transaction (CIT)

A Transaction in which the Cardholder actively participates by presenting a Card or Access Device at the POI or agreeing to the use of a Stored Credential to complete the Transaction, and may be required to perform a CVM or other Cardholder authentication.

Chip-only MPOS Terminal

An MPOS Terminal that has a contact chip reader and no magnetic stripe-reading capability and that must:

1. Operate as an online-only POS Terminal for authorization purposes;
2. Support either signature or No CVM Required as a Cardholder Verification Method, and may also support PIN verification if conducted by means of a PIN entry device (PED) that is in compliance with the Payment Card Industry (PCI) POS PED Security Requirements and Evaluation Program; and
3. Otherwise comply with the Corporation's requirements for Hybrid POS Terminals.

Chip Card (Smart Card, Integrated Circuit Card, IC Card, or ICC)

A Card with an embedded EMV-compliant chip containing memory and interactive capabilities used to identify and store additional data about a Cardholder, an Account, or both.

Chip Transaction

A Contact Chip Transaction or a Contactless Transaction.

Contact Chip Transaction

A Transaction in which data is exchanged between the Chip Card and the Terminal through the reading of the chip using the contact interface, in conformance with EMV specifications.

Contactless Payment Device

A means other than a Card by which a Cardholder may access an Account at a Terminal in accordance with the Standards. A Contactless Payment Device is a type of Access Device that exchanges data with the Terminal by means of radio frequency communications. Also see Mobile Payment Device.

Contactless Transaction

A Transaction in which data is exchanged between the Chip Card or Access Device and the Terminal through the reading of the chip using the contactless interface, by means of radio frequency communications. Also see EMV Mode Contactless Transaction, Magnetic Stripe Mode Contactless Transaction.

Corporation

Mastercard International Incorporated, Maestro International Inc., and their subsidiaries and affiliated entities. As used herein, Corporation also means the President and Chief Executive Officer of Mastercard International Incorporated, or his or her designee, or such officers or other employees responsible for the administration and/or management of a program, service, product, system or other function. Unless otherwise set forth in the Standards, and subject to any restriction imposed by law or regulation, or by the Board of Directors of Mastercard International Incorporated, or by the Mastercard International Incorporated Certificate of Incorporation or the Mastercard Incorporated Certificate of Incorporation (as each such Certificate of Incorporation may be amended from time to time), each such person is authorized to act on behalf of the Corporation and to so act in his or her sole discretion.

Credential-on-file Transaction

A Transaction initiated at a Merchant location with a Stored Credential, pursuant to the Cardholder's express authorization for the use of such Stored Credential to effect the Transaction.

European Economic Area (EEA)

The following countries, islands, and territories: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Canary Islands, Ceuta, Melilla, Azores, Madeira, Aland Islands, Jan Mayen, French Guiana, Guadeloupe, Martinique, Réunion, Saint Martin (French Part), and Mayotte.

For the sake of clarity, the EEA does not include: Andorra, Monaco, San Marino, Switzerland, Vatican City, Antarctica, Greenland, Faroe Islands, Akrotiri and Dhekelia, Saint Pierre and Miquelon, Saint Barthélemy, Saint Martin (Dutch Part), Svalbard, United Kingdom, Gibraltar, Falkland Islands, Channel Islands, Isle of Man, Pitcairn, Henderson, Ducie and Oeno Islands, Saint Helena, Ascension and Tristan da Cunha, South Georgia and the South Sandwich Islands.

European Union (EU)

The following countries, islands, and territories: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Canary Islands, Ceuta, Melilla, Azores, Madeira, Aland Islands, French Guiana, Guadeloupe, Martinique, Réunion, Saint Martin (French Part), and Mayotte.

Hybrid Terminal

A Terminal, including any POS or MPOS Terminal ("Hybrid POS Terminal," "Hybrid MPOS Terminal"), ATM Terminal ("Hybrid ATM Terminal"), or Bank Branch Terminal ("Hybrid Bank Branch Terminal"), that:

1. Is capable of processing both Contact Chip Transactions and magnetic stripe Transactions;
2. Has the equivalent hardware, software, and configuration as a Terminal with full EMV Level 1 and Level 2 type approval status with regard to the chip technical specifications; and
3. Has satisfactorily completed the Corporation's Terminal Integration Process (TIP) in the appropriate environment of use.

Issuer

A Customer in its capacity as an issuer of a Card or Account.

Manual Cash Disbursement Transaction

A disbursement of cash performed upon the acceptance of a Card by a Customer financial institution teller. A Manual Cash Disbursement Transaction is identified with MCC 6010 (Manual Cash Disbursements—Customer Financial Institution).

Marks

The names, logos, sounds, haptics, visual depictions, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks that the Corporation owns, manages, licenses, or otherwise Controls and makes available for use by Customers and other authorized entities in accordance with a License. A "Mark" means any one of the Marks.

Mastercard Switching Services

The Mastercard Division which provides Network Activities within the EEA, United Kingdom/ Gibraltar including its officers and/or other employees responsible for the administration and/or management of a service, system or other function. Subject to any restriction imposed by law or regulation, each such person is authorized to act on behalf of Mastercard Switching Services and to so act in his or her sole discretion.

Merchant

A retailer, or any other person, firm or corporation that, pursuant to a Merchant Agreement, agrees to accept Cards when properly presented.

Merchant Country of Origin

The Acquirer must populate the Merchant Country of Origin in each Transaction conducted by a Government Controlled Merchant, whether such country is the same as or different from the country in which the Merchant is located or the Transaction occurs in DE 48 (Additional Data: Private Use), subelement 37 (Additional Merchant Data), subfield 4 (Home Country ID) of Authorization Request/0100, Authorization Advice/0120, and Reversal Request/0400 messages and in PDS 0213 (Home Country ID) in First Presentment/1240 messages.

Merchant-initiated Transaction (MIT)

A Card-not-present Transaction that a Merchant initiates based on a prior agreement with the Cardholder, and in which the Cardholder does not actively participate. An MIT may be a recurring payment (standing order, subscription, unscheduled COF, or installment payment) or industry practice (partial shipment, related/delayed charge, no-show, or resubmission).

Mobile POS (MPOS) Terminal

An MPOS Terminal enables a mobile device to be used as a POS Terminal. Card "reading" and software functionality that meets the Corporation's requirements may reside within the mobile device, on a server accessed by the mobile device, or in a separate accessory connected (such as via Bluetooth or a USB port) to the mobile device. The mobile device may be any multi-purpose mobile computing platform, including, by way of example and not limitation, a feature phone, smart phone, tablet, or personal digital assistant (PDA).

Mobile Payment Device

A Cardholder-controlled mobile device containing a Payment Application compliant with the Standards, and which uses an integrated keyboard and screen to access an Account. A Mobile Payment Device may also be a Contactless Payment Device or a Mastercard Consumer-Presented QR payment device.

Network

The computer hardware and software operated by and on behalf of Mastercard Switching Services for the routing, switching, and settlement of Transactions including, without limitation, the Mastercard ATM Network, the Dual Message System, the Global Clearing Management System (GCMS), and the Settlement Account Management (SAM) system.

Network Activity(ies)

The undertaking of authorization, clearing and settlement using the Network.

Network Participant

A financial institution or other entity that uses the Network for Network Activity. An Issuer or an Acquirer are Network Participants.

Payment Application

A package of code and data stored in a Card, an Access Device, a server, or a combination of Access Device and server, that when exercised outputs a set of data that may be used to effect a Transaction, in accordance with the Standards. A Mastercard Payment Application, Maestro Payment Application, and Cirrus Payment Application is each a Payment Application.

Point of Interaction (POI)

The location at which a Transaction occurs or a PTA Transaction originates, as determined by the Corporation.

Point-of-Sale (POS) Terminal

- An attended or unattended device, including any commercial off-the-shelf (COTS) or other device enabled with mobile point-of-sale (MPOS) functionality, that is in the physical possession of a Merchant and is deployed in or at the Merchant's premises, and which enables a Cardholder to use a Card or Access Device to effect a Transaction for the purchase of products or services sold by such Merchant; or
- A Bank Branch Terminal. A POS Terminal must comply with the POS Terminal security and other applicable Standards.

Point–of–Sale (POS) Transaction

The sale of products or services by a Merchant to a Cardholder pursuant to acceptance of a Card by the Merchant or Manual Cash Disbursement Transaction. A POS Transaction may be a Card-present Transaction taking place in a face-to-face environment or at an unattended POS Terminal, or a Card-not-present Transaction taking place in a non-face-to-face environment (for example, an ecommerce, mail order, phone order, or recurring payment Transaction).

Rules

The Standards set forth in this manual.

Standards

The organizational documents, operating rules, regulations, policies, and procedures of the Corporation, including but not limited to any manuals, guides, announcements or bulletins, as may be amended from time to time.

Stand-In Parameters

A set of authorization requirements established by the Corporation or the Issuer that are accessed by the Interchange System using the Stand-In Processing

Stand-In Processing Service

A service offered by the Corporation in which the Interchange System authorizes or declines Transactions on behalf of and uses Stand-In Parameters provided by the Issuer (or in some cases, by the Corporation). The Stand-In Processing Service responds only when the Issuer is unavailable, the Transaction cannot be delivered to the Issuer, or the Issuer exceeds the response time parameters set by the Corporation.

Stored Credential

Mastercard or Maestro Account data (meaning PAN and expiration date) retained by a Merchant or its Acquirer in accordance with the Cardholder's express authorization for the Merchant to store such Account data (or a Tokenized replacement of the originally provided Account data generated by Merchant Card-on-File Tokenization) for use in future Transactions.

Terminal

Any attended or unattended device capable of the electronic capture and exchange of Account data that meets the Corporation requirements for Terminal eligibility, functionality, and security, and permits a Cardholder to effect a Transaction in accordance with the Standards. An ATM Terminal, Bank Branch Terminal, and POS Terminal is each a type of Terminal.

Transaction

A financial transaction arising from the proper acceptance of a Card or Account bearing or identified with one or more of the Brand Marks, either alone or in combination with the marks of another payment scheme, at a Card acceptance location and identified in messages with a Card Program identifier.

Notices

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

Proprietary Rights

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

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

Trademarks

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

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

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

Disclaimer

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

Translation

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

Information Available Online

Mastercard provides details about the standards used for this document, including times expressed, language use, and contact information, on the Technical Resource Center (TRC). Go to the Rules collection of the References section for centralized information.