AN 2993 Reminder of Mastercard Rule 1.2 for Anti-Money Laundering and Sanctions Requirements

Type:
Bulletin Announcement

Category:
Operations
Rules/Standards

Audience:
Acquirer
Issuer
Processor

Region:
Global

Brand:
Mastercard®
Debit Mastercard®
Maestro®
Cirrus®
Mastercard Electronic™
U.K. Domestic Maestro™

Action Indicator:
Brand Mandate
Network Mandate

Published:
9 November 2021

Effective:
9 November 2021

Executive Overview

Mastercard is reminding customers that, at all times, license applicants and customers must maintain a comprehensive Anti-Money Laundering (AML) and Sanctions Compliance Program that safeguards Mastercard and the Interchange System.

Effective date details

Date	Details
9 November 2021	Reminder to customers of Anti-Money Laundering (AML) and Sanctions Compliance Program safeguards

Customer benefit

Customers will benefit from this reminder by ensuring they maintain a comprehensive Anti-Money Laundering (AML) and Sanctions Compliance Program.

What Mastercard is doing

Mastercard reminds all license applicants and customers that under Rule 1.2 "Mastercard Anti-Money Laundering and Sanctions Requirements" (Mastercard Rule 1.2) of the *Mastercard Rules* manual for AML and sanctions requirements, all must ensure their Mastercard activity does not violate relevant AML laws and regulations, as well as Mastercard Standards.

Version history

Date	Description of change
9 November 2021	Update to format Added text to the Rule 1.2. Requirements reminding Customers to have Transaction Monitoring Rules for ATM acquiring activity
9 January 2020	Added text to the Rule 1.2. Requirements to remind customers to comply with requests for information and/or documents from the Global AML Compliance Team
3 October 2019	Initial publication date

Rule 1.2.1 Anti-Money Laundering Requirements

Per Rule 1.2.1 "Anti-Money Laundering Requirements" of the *Mastercard Rules* manual, license applicants and customers are obligated to have a written AML compliance program with a policy, procedures, and controls in place to safeguard Mastercard and the Interchange System from money laundering, terrorist financing, or both.

Each license applicant's and customer's AML compliance program must be commensurate with its respective AML risk profile and fully implemented in accordance with this rule and local regulatory requirements.

A license applicant's and customer's AML compliance program must address, in a manner satisfactory to Mastercard, all activity and include, at a minimum, the following:

- A process to ensure thorough client identification and due diligence.
- Sufficient controls, resources, and monitoring systems for the prompt detection and reporting of suspicious activity.
- Compliance with all regulatory record-keeping and reporting requirements.
- Risk assessment processes designed to identify and apply appropriate risk management controls.
- A training program for all personnel whose duties require knowledge of the AML compliance program and requirements.
- An independent audit process to periodically test controls.

Rule 1.2.2 Sanctions Requirements

Per Rule 1.2.2 "Sanctions Requirements" of the *Mastercard Rules* manual, each customer, regardless of where situated, must ensure that activity is in compliance with the sanctions laws and regulations enacted by United States sanctions authorities (including, the United States Office of Foreign Assets Control [OFAC] and the United States Department of State), as well as all applicable local sanctions regulations where the activity is taking place.

A customer is prohibited from engaging in activity with any person, including any legal entity or government, or in any geography in contravention of any regulation or other requirement promulgated by the United States sanctions authorities, as well as any applicable local sanctions authority. Each customer engaging in or proposing to engage in activity must have a written sanctions compliance program that includes a policy, practices, procedures, and controls. The sanctions compliance program must address, to the satisfaction of Mastercard, all activity and include, at a minimum, the following.

- Screening:
  1. An issuer must screen its cardholders and/or service providers and other representatives and agents (including, but not limited to, a program manager) at the time of onboarding and on an ongoing basis,

against applicable sanctions lists, including, but not limited to, OFAC sanctions lists (such as, the Specially Designated Nationals and Blocked Persons List [SDN List]).

2. An acquirer must screen its merchants and service providers and other representatives and agents (including, but not limited to, a third party processor [TPP]) at the time of onboarding, and on an ongoing basis, against applicable sanctions lists, including, but not limited to, OFAC sanctions lists [such as, the SDN List]).

- Prohibited Activity:
  1. No activity may be conducted in a geography (country or region) that is the subject of applicable sanctions, such as those identified by OFAC. No activity may be conducted with a person, entity, or government (including a Government Controlled Merchant) on the OFAC sanctions lists (such as, the SDN List). A customer must immediately cease any activity with a person, entity, or government (including a Government Controlled Merchant) identified as listed on any of the OFAC sanctions lists.

Government Controlled Merchant: A merchant that is a government entity or an entity that is at least 50 percent owned or controlled (either directly, indirectly, legally or beneficially) by a government or government entity.

NOTE: Activity with an entity listed on OFAC's Sectoral Sanctions Identifications List (SSI List) may only be conducted in compliance with the limitations or conditions established by OFAC for that program.

Transaction Monitoring Required for ATM Acquirers

ATM Acquirers are obligated under Mastercard Rule 1.2 to monitor and report suspicious ATM activity, regardless if the issuer has or has not reported the activity as fraud. An ATM Acquirer including their service providers, agents or other third parties acting on their behalf, must have sufficient controls, resources and monitoring systems for the prompt detection and reporting of suspicious ATM activity. Please refer to Mastercard's *Security Rules and Procedures* for additional information.

As part of Mastercard's Customer Due Diligence process, the Global Anti-Money Laundering Compliance Team conducts periodic reviews which may require additional information relating to transactional activity, forms to be completed, or documentation to be provided to evaluate a customer's Anti-Money Laundering and Sanctions Program. This evaluation may include, but is not limited to, a request for detailed information about one or more of the following; the customer, its activities, its AML procedures and controls, or the identity of its owners, directors, and senior executives.

Each customer must fully cooperate with inquiries, periodic reviews and any other efforts undertaken by the corporation to evaluate a customer's compliance with Rule 1.2 of the *Mastercard Rules*. Such requests may be initiated to confirm that a customer or service provider does not pose undue risk to Mastercard.

Mastercard reserves the right to conduct an AML or Sanctions onsite review of customers and service providers at any time.

Noncompliance Violations

Customers failing to comply with any requirement under Rule 1.2 or failing to respond to any request for information or documentation as required under Rule 3.9 "Obligation of Customer to Provide Information" of the *Mastercard Rules*, may be subject to a noncompliance assessment and/or other disciplinary actions, including but not limited to implementation of a full or partial suspension of a customer's Mastercard activities.

Mastercard may deem the customer's noncompliance with Rule 1.2 requirements to pose significant money laundering, terrorist financing and sanctions risk to the Mastercard system, its customers, or other stakeholders and may take necessary action as stated previously.

Any violation of Rule 1.2 of the *Mastercard Rules* manual can result in serious consequences. Violations that come to the attention of Mastercard can result in possible fines or assessments, the suspension or termination of a license, in addition to other action Mastercard may deem necessary and appropriate.

Third Party Service Providers

License applicants and customers must ensure that in the event customers engage third party service providers to perform any AML or sanctions compliance responsibilities on their behalf, customers must maintain strict oversight and monitoring of the third party service providers to ensure the Mastercard activity does not violate relevant, local AML laws and regulations, as well as Mastercard Standards.

Customers are responsible for all service providers and must have documented procedures detailing oversight controls which include, but are not limited to, the due diligence performed at onboarding of the third party service provider, the ongoing monitoring to ensure the third party service provider is in compliance with Rule 1.2 of the *Mastercard Rules* manual at all times, and an audit process to test those controls.

All third party service providers must be appropriately registered with Mastercard.

Merchants

License applicants and customers engaging in acquiring activity must ensure that their AML compliance program is applied to all merchants and sub-merchants, retailers, firms, persons, or corporations selling goods or services (seller) and ATM owners from which it acquires transactions, whether such transactions are submitted to the customer directly by the seller or ATM owner or through a service provider acting for or on behalf of such customer.

Each acquirer, before entering into a merchant agreement with a merchant, must conduct thorough due diligence as per their AML program and the Mastercard Standards to verify that the prospective merchant is a bona fide business.

Procedures for verifying that a merchant or ATM owner is a bona fide business are set forth in Chapter 7 of the *Security Rules and Procedures* manual.

Each acquirer must capture appropriate identifying details about each merchant, such as full legal name or location as per their AML program and the Mastercard Standards. Mastercard Standards related to acquiring activity are outlined, in part, in the Transaction Processing Rules, as well as in Chapter 5 of the *Mastercard Rules* and Chapter 6 of the Security Rules and Procedures, which contains rules relating to merchant and ATM owner agreements, acquirer and merchant obligations, and card acceptance requirements.

The aforementioned obligations must be captured in a documented policy and or procedure and must be available for review by Mastercard upon request.

Questions

Customers with questions about the information in this announcement should contact Global Customer Service using the contact information on the Technical Resource Center.

Mastercard Global AML Compliance Group

Email: aml_program@mastercard.com