GLB 10971.2 Revised Standards for the Merchant Monitoring Program

Type:
Bulletin announcement

Category:
Rules/Standards

Audience:
Acquirer
Branded Processor
Processor
Network Enablement Partner

Region:
Global

Brand:
Mastercard®
Debit Mastercard
Maestro®

Action indicator:
Opt-in

Published:
17 June 2025

Effective:
14 January 2025

Executive overview

Mastercard previously announced it was revising the Standards to clarify customer obligations relating to the Merchant Monitoring Program.

Effective date details

Date	Details
14 January 2025	Revised standards are effective

Customer benefit

Mastercard is encouraging customers to proactively monitor for and prevent transaction activity that is fraudulent, illegal, or brand-damaging, in violation of the Business Risk Assessment and Mitigation (BRAM) program, or involves merchant transaction laundering (where a merchant account is used to submit such transactions for or on behalf of a third party). An acquirer that opts to participate in the Merchant Monitoring Program must engage one or more Merchant Monitoring Service Providers (MMSPs) to perform BRAM monitoring and merchant transaction laundering detection services on the acquirer's behalf.

The revised Standards clarify customer obligations under the Merchant Monitoring Program, as described in Section 8.9 of the *Security Rules and Procedures* manual.

What Mastercard is doing

Mastercard is clarifying that these obligations must include the outlined to ensure that:

- Mastercard approves the registered MMSP to perform BRAM monitoring and merchant transaction laundering detection services
- The MMSP conducts an initial merchant scan to identify potential BRAM content, products, or services, or merchant transaction laundering, before the start of transaction processing
- Merchant URLs monitoring is continuous and complete, which explicitly includes any restricted members-only areas; and
- The MMSP itself generates each monthly report provided to Mastercard relating to the MMSP's merchant monitoring and identification of violations, and authors each MMSP incident report created as part of the acquirer's response to a BRAM notification. If submitted to Mastercard directly by the acquirer, each monthly report and each incident report must be an unaltered copy of the report generated by the MMSP; and
- Each monthly report outlines each acquirer's merchants and must ensure each is monitored by the MMSP.

Version history

Date	Description of change
17 June 2025	Updated revised Standards to: • Include a requirement for the MMSP to conduct an initial merchant scan before transaction acquiring begins • Clarify that URL monitoring must include restricted members-only areas, unless such monitoring is prohibited by law.
14 January 2025	Initial publication date

Acquirer impact

To participate in the Merchant Monitoring Program, an acquirer must complete the following.

- Register an MMSP as its service provider
- Submit to the MMSP all merchant information and additional data that the MMSP deems necessary or appropriate
- Ensure that the MMSP persistently monitors each merchant's activity to identify potential BRAM violations and merchant transaction laundering
- Require the MMSP to report all identifications of potential merchant violations to the acquirer within five business days
- Within 15 calendar days of receiving MMSP notification of an identification, investigate the potential violation, ensure that all violating activity has ceased, and report the resolution of the identification to the MMSP
- Provide Mastercard with monthly reports of monitored merchants and violations identified by the MMSP during that time (submitted either directly by the MMSP or by the acquirer)
- Adhere to the standards for use of the Merchants to the Mastercard Alert To Control High-risk Merchants (MATCH) system, when applicable

Overview of revised Standards

Mastercard is revising the Standards relating to customer obligations for participation in the Merchant Monitoring Program, as outlined in Section 8.9 of the *Security Rules and Procedures* manual.

Revised Standards

To view the revision, refer to the attachment associated with this bulletin announcement, which shows underlining for additions and strikethrough for deletions.

Related information

- *Security Rules and Procedures*

Questions

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