Revised Standards for the Merchant Monitoring Program

Mastercard is revising the Standards announced in the article *GLB 10971 Revised Standards for the Merchant Monitoring Program*.

Overview of revised Standards

Customers should review the revisions to the publication in this document and make appropriate plans to support the revised Standards.

Effective date	Changes to Standards in...	Will be published in...
14 January 2025	*Security Rules and Procedures*	Chapter 8 Mastercard Fraud Control Programs

Mastercard will incorporate the revised Standards into a future edition of the manual. The manual is available in the Technical Resource Center on Mastercard Connect™.

Revised Standards for *Security Rules and Procedures*

Mastercard will revise the *Security Rules and Procedures* to include these Standards. Additions to the Standards are underlined. Deletions are indicated with a ~~strikethrough~~.

Chapter 8 Mastercard Fraud Control Programs

8.9 Merchant Monitoring Program (MMP)

Mastercard encourages Customers to proactively monitor for and prevent BRAM violations and Merchant Transaction laundering. An Acquirer that chooses to participate in the Merchant Monitoring Program must engage one or more Merchant Monitoring Service Providers (MMSPs) to perform BRAM monitoring and/or Merchant Transaction laundering detection services on the Acquirer's behalf.

Mastercard maintains a list of vendors approved to perform MMSP Program Services, as described in *Mastercard Rules* section 7.1. For a current list of approved vendors, or

for information on how to become an approved vendor, send an email to MMP@mastercard.com.

8.9.1 MMP Participation Requirements

To participate in the Merchant Monitoring Program, an Acquirer must:

- Confirm the MMSP has been approved by Mastercard to perform BRAM monitoring and/or Merchant Transaction laundering detection services;
- Register the MMSP as its Service Provider as described in *Mastercard Rules* section 7.10;
- Submit to the MMSP all Merchant information and any additional data that the MMSP deems necessary or appropriate for the successful monitoring of the particular Merchant (including the Merchant legal name, Merchant "doing business as" name, Merchant address, and all Merchant URLs);
- Ensure that the MMSP conducts an initial scan of the Merchant's activity for the purpose of identifying potential Merchant violations related to BRAM content, products, or services and/or Merchant Transaction laundering prior to accepting Transactions from the Merchant;
- Ensure that the MMSP persistently monitors each Merchant's activity for the purpose of identifying potential Merchant violations related to BRAM content, products and services and/or Merchant Transaction laundering;
- Ensure Merchant URLs are monitored completely, which explicitly includes any restricted members-only areas where products, digital content, and/or services are offered, unless such monitoring is prohibited by law;
- Require the MMSP to report all identifications of potential Merchant violations to the Acquirer within five (5) 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 generated by the MMSP detailing all of its Merchants being monitored as part of the MMP and all violations identified by the MMSP during that time. A report submitted to Mastercard directly by the Acquirer must be an unaltered copy of the report generated by the MMSP. The reports may be submitted by the MMSP on the Acquirer's behalf; and
- Adhere to the MATCH Standards set forth in Chapter 11, when applicable

If an Acquirer receives a BRAM notification from Mastercard regarding a Merchant that is being monitored as part of the MMP, the Acquirer must provide an ~~MMSP Incident Report~~ incident report authored by the MMSP as part of its response to the BRAM notification. An incident report submitted to Mastercard directly by the Acquirer

must be an unaltered copy of the report generated by the MMSP. The report must include:

- The date on which the Acquirer provided the Merchant information to the MMSP;
- Confirmation that the Merchant was persistently monitored;
- The dates and contents of any alerts that the MMSP generated and sent to the Acquirer during the monthly period in which the BRAM notification occurred, and any response or action taken by the Acquirer;
- How and why the BRAM violation was not detected by the MMSP;
- How the MMSP will ensure the detection of future potential Merchant violations of a similar nature.

8.9.2 MMP Monthly Reporting Format and Submission

The following requirements apply with respect to each monthly report:

- The report must list all of the Acquirer's Merchants that are being persistently monitored by the MMSP.
- The report must be provided as a Microsoft Excel file that is formatted and prepared as follows. All required data fields must be complete and accurate.
    - Acquirer name and ICA number
    - MMSP name
    - Report submitter contact name and email address
    - Merchant name
    - Merchant URL(s)
    - Date the Merchant information, including URL, was provided to the MMSP
    - Merchant MCC
    - Applicable MMSP service(s)
    - Violation type, if applicable
    - Violation category, if applicable
    - URL content details
    - Date MMSP violation reported to Acquirer, when applicable
    - Date Acquirer resolved and reported to MMSP, when applicable
    - Investigation findings and final resolution status, when applicable

- Each file must utilize a standard naming convention, as follows (where NNNNNN is the Acquirer ICA): NNNNNN Acquirer Name - Service Provider Name - MMSP Name - Date of Report
- Separate files must be prepared for each Acquirer ICA or Acquirer legal entity name. Merchant activity acquired under the specified Acquirer ICA or Acquirer legal entity name must be the only data contained in that file.
- Submit each report attached to an email message to mmp@mastercard.com or as otherwise approved by Mastercard. The maximum email attachment size is 20 MB. Attachments that exceed this size should be split into multiple attachments (each in a separate email message), so that no single attachment is larger than 20 MB.

The Acquirer is responsible for ensuring that Mastercard receives the monthly report within 30 days of the completion of monitoring for a given month (for example, by July 1 for monitoring during the period of May 1 through May 31).

8.9.3 Eligibility for Assessment Mitigation

~~An~~ With respect to an Acquirer that fully participates in the MMP and that processes Transactions for a Merchant that has undergone an initial scan prior to the first Transaction and is being persistently monitored by a MMSP for any identifications related to BRAM content, products, and services and/or Merchant Transaction Laundering, Mastercard may provide mitigations as outlined below and as applicable to assessments related to violations of the BRAM Rules or Merchant Agreement Rule (collectively referred to as "BRAM activity").