AN 2968—Revised Standards—Data Integrity Monitoring Program—Introducing the Acquirer Chargeback Monitoring Program

Generated on 22 January 2020

Published on 21 January 2020

AN 2968—Revised Standards—Data Integrity Monitoring Program—Introducing the Acquirer Chargeback Monitoring Program

Mastercard is announcing a new program to monitor acquirer chargeback data through the Data Integrity platform.

Version History

The version history of this announcement is as follows.

Date	Description of Change
21 Jan 2020	• Changed the title of the bulletin announcement from "AN 2968—Revised Standards—Data Integrity Monitoring Program—Introducing the Acquiring Chargeback Program" to "AN 2968—Revised Standards—Data Integrity Monitoring Program—Introducing the Acquirer Chargeback Monitoring Program" • Changed the bulletin announcement's regional scope to Global as the announcement now applies to the Asia/Pacific region as well (The change can be found in the At-a-Glance table) • Revised the assessments effective date from 1 April 2020 to 1 May 2020 • Added edit clarification information in the "Overview" section • Added clarifications for the Canada region in the "Comply-By Date and Noncompliance Assessments" section • Changed the references to EFM in Table 2 and Table 3 to ECM in the "Overview" and "Comply-By Date and Noncompliance Assessments" sections respectively • Changed the references to ECP in Table 6 and Table 7 to ECM in the "Comply-By Date and Noncompliance Assessments" section • Added clarification for extension
29 Oct 2019	Initial publication date

At-A-Glance

The At-A-Glance table provides key information about the systems and groups affected by this announcement, action indicators that specify the appropriate action, and the required implementation date or dates.

Type:	Bulletin Announcement
Audience:	Acquirer, Issuer, Processor
	Each customer must independently determine the impact on its operations.
Brands:	Mastercard®, Debit Mastercard®, Maestro®
Regions:	Global
System:	Clearing
Category:	Rules/Standards, Operations, Pricing/Fees
Action Indicator:	Attention warranted (Program/service-related)
	Financial impact
	Registration required

Effective Date:	1 October 2019—Monitoring Begins 1 April 2020—Comply-By Date 1 May 2020—Assessments Begin

Overview

Mastercard is introducing the Acquirer Chargeback Monitoring Program, which will include two new edits.

The edits measure compliance at the merchant ID level (Data Element [DE] 42 [Card Acceptor ID Code]) and notify acquirers when a merchant ID has breached compliance thresholds. The edits are as follows:

Edit 1—Excessive Fraud Merchant

Edit 1—Excessive Fraud Merchant (EFM)—was originally announced in April 2019 as part of North America Assurance Framework ("AN 2530—U.S. Assurance Framework" and "AN 2819—Canada Assurance Framework"), and will now be deployed globally ("AN 2852 Revised Standards—Excessive Fraud Merchant Compliance Program"). The goal of the EFM program is to reduce fraud on electronic commerce (e-commerce) transactions, creating a more secure ecosystem and providing a better experience for cardholders. The EFM program will measure compliance at the merchant ID level and send the notifications and potential financial assessments to their acquirer.

Merchants in the following countries are excluded from the EFM Program:

- Ascension and Tristan Da Cunha
- Germany
- India
- Liechtenstein
- St. Helena
- Switzerland

Refer to the following table for EFM monthly criteria information.

Table 1. EFM Monthly Criteria

Number of Electronic-Commerce Transactions	Fraud Chargeback Amount	Fraud Chargeback Basis Points	3DS Utilization (including Data Only Transactions)
1,000 or more	EUR/USD 50,000 or more	50 or more	• Less than 10% (Non-regulated Countries) • Less than 50% (Regulated Countries)

Edit 2—Excessive Chargeback Merchant

Edit 2—Excessive Chargeback Merchant (ECM) is part of an update to the Excessive Chargeback Program (ECP), which monitors merchants that receive an excessive number of chargebacks on a monthly basis. Merchants will be evaluated under two categories—Excessive Chargeback Merchant (ECM) and High Excessive Chargeback Merchant (HECM). Going forward, Mastercard will automatically track chargebacks for all transactions, including e-commerce transactions, through network data, and notify acquirers when an individual merchant ID has breached the compliance threshold. ECM is intended to reduce chargebacks and strengthen the integrity of the Mastercard Network.

Refer to the following table for ECM and HECM monthly criteria information.

Table 2. ECM and HECM Monthly Criteria

Monthly Criteria	Number of Chargebacks	Basis Points
ECM	100 to 299	150 to 299
HECM	300 or more	300 or more

Data Integrity Monitoring Program and Mandatory Use of Data Integrity Online

The Data Integrity Monitoring Program monitors transactions to promote data quality and performs systematic validations to help ensure that customers:

- Process transactions according to Mastercard processing rules, requirements, and standards
- Adhere to product and service mandates as applicable

As the industry continues to evolve, the criticality of acquirer compliance is increasingly paramount in Mastercard's efforts to dismantle fraud, increase approval rates, and reduce chargebacks.

Customers can view their compliance data and receive notifications of noncompliance through the Data Integrity Online application on Mastercard Connect™. Registration for this application is mandatory for every ICA and processor ID, and Mastercard will assess customers against all applicable edits even if the customer has not registered a user.

Note:

Effective 1 October 2018, notifications of noncompliance are sent to the System Administrator for ICAs that do not have a registered user in Data Integrity Online.

Comply-By Date and Noncompliance Assessments

Monitoring for both edits in the Acquirer Chargeback Monitoring Program will begin 1 November 2019 to identify violations that occurred in October 2019. Customers will be provided a six-month transition period for all countries except Canada, which has an eleven month transition period, before any fees are assessed through Data Integrity.

This program does not apply to merchants in Ascension and Tristan Da Cunha, Germany, India, Liechtenstein, St. Helena, and Switzerland.

Note:

Acquirers must continue to monitor their merchants and report chargeback levels to Mastercard through the Mastercard Registration Program (MRP) for all merchants exceeding the existing ECP thresholds during the transition period as noted previously. For all countries except Canada reporting through MRP and assessments will continue under the existing program through the violation month of March 2020. For Canada, reporting through MRP and assessments will continue under the existing program through the violation month of August 2020.

Compliance status and reporting will also be available on the Data Integrity Online application on Mastercard Connect. Within applicable countries, any merchant ID that remains noncompliant with the EFM or ECM criteria after the transition period ends will be assessed according to the assessment structure for each edit as outlined in the Data Integrity Monitoring Program manual, based upon the noncompliance activity during the transition period.

Mastercard will start monitoring in November 2019 for the October 2019 violation month and will start charging assessments in May 2020 (except Cananda) based on the number of months in the Aquirer Chargeback Monitoring Program as of the April 2020 violation month. The transition period is for all merchant activity during these months, regardless of the number of violations during that time period. The transition period will not be extended beyond the April 2020 violation month (except Canada) however a customer may request an extension.

For merchants in Canada, Mastercard will start charging assessments in October 2020 based upon the number of months in the ACMP as of the September 2020 violation month.

Refer to the following table for an example of a merchant ID exceeding ECM status in October 2019.

Table 3. Merchant ID Exceeding ECM Status in October 2019

Violation Month	**ECM Status**	**Assessment Amount**
October 2019	ECM (month 1)	0
November 2019	ECM (month 2)	0*
December 2019	ECM (month 3)	0*
January 2020	ECM (month 4)	0*
February 2020	ECM (month 5)	0*
March 2020	ECM (month 6)	0*
April 2020	ECM (month 7)	EUR/USD 25 000

*Assessment amount waived during six month transition period. In the aforementioned example, a total of EUR/USD 17,000 was waived during the transition period.

The following dates apply.

Table 4. Applicable Dates

	Notifications Begin	**Comply-By Date**	**Assessments Begin**
Global (except Canada)	1 November 2019	1 April 2020	1 May 2020
Canada	1 November 2019	1 September 2020	1 October 2020

The following assessment structure will apply to EFM identifications in applicable countries.

Table 5. **EFM Assessment Structure**

Number of Months Above ECM Thresholds	**Violation Assessment**
1	0
2	EUR/USD 500
3	EUR/USD 1,000
4 to 6	EUR/USD 5,000

7 to 11	EUR/USD 25,000
12 to 18	EUR/USD 50,000
19+	EUR/USD 100,000

The following assessment structure will apply to ECM identifications.

Table 6. ECM Assessment Structure

Number of Months Above ECM Thresholds	Assessment if ECM in Violation Month (100–299 Chargebacks and 150–299 Basis Points)	Assessment if High Excessive Chargeback Merchant (HECM) in Violation Month (Greater than 300 Chargebacks and Greater than 300 Basis Points)	
	Violation Assessment	**Violation Assessment**	**Issuer Recovery Assessment**
1	0	0	No
2	EUR/USD 1,000	EUR/USD 1,000	No
3	EUR/USD 1,000	EUR/USD 2,000	No
4 to 6	EUR/USD 5,000	EUR/USD 10,000	Yes*
7 to 11	EUR/USD 25,000	EUR/USD 50,000	Yes*
12 to 18	EUR/USD 50,000	EUR/USD 100,000	Yes*
19+	EUR/USD 100,000	EUR/USD 200,000	Yes*

*Issuer recovery assessment applies at EUR/USD 5 per chargeback over 300 chargebacks. For example, a merchant with 500 chargebacks would be assessed EUR/USD 1,000 in issuer recovery (500-300 = 200 x EUR/USD 5 = EUR/USD 1,000)

A merchant's status in the Acquirer Chargeback Monitoring Program does not reset as compliant, until the merchant ID has achieved three consecutive months below the program thresholds.

Table 7. Example of ECM/HECM Status Reset

Month	ECM Status	Assessment Amount
January	ECM (month 1)	0
February	No Violation	0
March	ECM (month 2)	EUR/USD 1,000
April	HECM (month 3)	EUR/USD 2,000
May	No Violation	0
June	No Violation	0
July	No Violation—Audit Closed	0

Extension Requests

Customers may request an extension through the edit tile in the Data Integrity Online application for individual merchant IDs that are unable to comply with the edit requirements. Extensions are reviewed and granted on a case-by-case basis. Mastercard may request additional information, such as an action plan, to evaluate an extension request.

Customers should request extensions for merchants that quickly addressed the circumstances that caused identification in the Acquirer Chargeback Monitoring Program. An extension will allow ample time for the remaining chargebacks to be processed and the merchant to return to compliance with program thresholds. This extension request process replaces previous requests, in the former ECP program, to apply mapped back data.

If a merchant ID successfully complies with edit requirements for three consecutive months before the extension period ends, assessments will not apply. However, if a merchant ID receives approval for an extension request, compliance must be achieved by the end of the extension period, or the customer will be retroactively billed for any assessments they would have accrued during the time the extension was in place.

The customer will also be retroactively billed for any assessments they would have accrued during the time the extension was in place if the merchant ID is terminated (for example, zero sales are processed by the merchant ID in a calendar month) before the end of the extension period and/or does not successfully exit the program by having three consecutive months below the program thresholds.

Once three consecutive months below the program thresholds have been met, future violations for the same merchant ID will be treated as first-time noncompliance under the applicable edit assessment structure.

Any merchant ID identified as noncompliant for both EFM and ECM in the same month will only be subject to the applicable EFM assessments.

Edit Criteria

Edit Criteria is as follows.

Program: Acquirer Chargeback Monitoring

Table 8. Edit 1

Edit Number	**1**
Edit Title	Excessive Fraud Merchant
Name	Excessive Fraud Merchant
Billing Code	2DC0400
Region(s)	Global
Description	This edit monitors the total amount of fraud occurring at a given e-commerce merchant as well as the number of transactions authenticated through 3-D Secure (3DS).
Edit Criteria	Merchants are considered noncompliant when all of the following conditions are met in a given month: 1. The total dollar amount (or local currency equivalent) of fraud-related chargebacks exceeds EUR/USD 50,000 2. The total number of fraud chargeback basis points (bps) is greater than 50 3. The percentage of monthly clearing volume processed using 3DS (including Data Only transactions) is less than 10 percent in non-regulated countries, or less than 50 percent in regulated countries

Edit Number	**1**
	Note: Monthly fraud-related chargebacks are defined as those chargebacks processed within a calendar month under either of the following reason codes: • 4837 (No Cardholder Authorization) • 4863 (Cardholder Does Not Recognize-Potential Fraud) 3DS transactions are identified in clearing in private data subelement (PDS) 0052 (Security Level Indicators) with a value of 211, 212, 214, or 216. Data Only refers to non-3DS transactions in which Mastercard performs risk scoring and injects Digital Transaction Insights to the authorization request message. The term non-regulated refers to those countries without a legal or regulatory requirement for strong cardholder authentication. The term regulated refers to those countries with a legal or regulatory requirement for strong cardholder authentication. See appendix for full list. This program does not apply to merchants in Ascension and Tristan Da Cunha, Germany, India, Liechtenstein, St. Helena, and Switzerland.
Baseline/Threshold	Baseline: 1,000 e-commerce transactions in Clearing Threshold: N/A
Reference	Chargeback Guide

Table 9. Edit 2

Edit Number	**2**
Edit Title	Excessive Chargeback Merchant
Name	Excessive Chargeback Merchant
Billing Code	2DC0401 and 2DC0402
Region(s)	Global
Description	This edit monitors chargeback performance at the merchant ID level to determine if a merchant has exceeded monthly chargeback thresholds.
Edit Criteria	Merchants will be evaluated under two categories, Excessive Chargeback Merchant (ECM) and High ECM (HECM). Merchants are considered noncompliant in the ECM category when both of the following are true: • The total number of chargebacks is greater than 100 • The total number of chargeback bps is greater than 150 Merchants are considered noncompliant in the High ECM category when both of the following are true: • The total number of chargebacks is greater than 300 • The total number of chargeback bps is greater than 300 A merchant identified as noncompliant for Edit 1—Excessive Fraud Merchant will not be assessed for Edit 2—Excessive Chargeback Merchant.

Edit Number	**2**
	Once a merchant ID is identified in the ECM edit, the merchant ID will continue to be monitored until there are three consecutive months below the ECM thresholds, at which time the ECM status resets. Monthly chargebacks are defined as all first presentment chargebacks with a processed date within the violation month. Bps are the number of chargebacks received by the acquirer for a merchant ID in a calendar month divided by the number of Mastercard transactions processed for the merchant ID in the preceding month, and then multiplied by 10,000.
Baseline/Threshold	N/A
Reference	Security Rules and Procedures (Section 8.3)

Revised Standards

To view marked revisions, refer to the attachment associated with this announcement. Additions are underlined; deletions are indicated with a strikethrough.

Questions?

Customers with questions about this bulletin announcement should send an email message to:

Customer Data Performance Team	
Email:	ps_data_integrity@mastercard.com

