

AN 3405—Revised Standards—Online Gambling Transactions

Type:

Bulletin Announcement

Category:

Operations, Rules/Standards, Security

Audience:

Acquirer
Issuer
Processor

Region:

Global

Brand:

Mastercard®
Debit Mastercard®

Release:

20.Q2

Action Indicator:

Brand Mandate
Network Mandate

Published:

30 March 2020

Effective:

17 July 2020

Executive Overview

Mastercard is revising rules to expand an existing mandate for online gambling to all applicable gambling card acceptor business codes (MCCs) and to provide additional options for authentication. Mastercard is updating an existing rule that requires acquirers of online gambling transactions to include the card validation code (CVC) 2 value of the Mastercard account in the authorization request message. This update is intended to promote the use of enhanced authentication tools and, in turn, reduce fraud.

¹

Effective Date Details

Date	Details
17 July 2020	

Version History

Date	Description of Change
30 Mar 2020	17 April 2020 effective dates will be deferred to 17 July 2020
	The announcement was converted into the new announcement format.
18 Dec 2019	Initial publication date

Updates to the Rules

The following updates will be applied to this rule:

- An acquirer of online gambling transactions must ensure that at least one of the following occurs with respect to each online gambling transaction authorization request message:
 - The CVC 2 value is populated

¹ Each customer must independently determine the impact on its operations.

- EMV^{®2} 3-D Secure (3DS) authentication has occurred
- With respect to a recurring payment transaction, Identity Check Insights (previously called Data Only) are shared
- An online gambling transaction is defined as a card-not-present transaction identified with any of the following MCCs:
 - MCC 7995 (Gambling Transactions)
 - MCC 7800 (Government Owned Lottery [U.S. Region Only])
 - MCC 7801 (Internet Gambling [U.S. Region Only])
 - MCC 7802 (Government Licensed Horse/Dog Racing [U.S. Region Only])
 - MCC 9406 (Government Owned Lottery [Specific Countries])

Acquirer Impact

Acquirers that use EMV 3DS or Identity Check Insights for online gambling transactions are no longer required to send the CVC 2 value in the authorization request message.

Use of CVC 2

If an online gambling merchant collects the CVC 2 value to comply with this requirement, the CVC 2 value must be provided in Data Element (DE) 48 (Additional Data—Private Use), subelement 92 (CVC 2) of the Authorization Request/0100 message.

Use of Identity Check Insights (Previously Called Data Only)

If an online gambling merchant shares Identity Check Insights to comply with this requirement when conducting a recurring payment transaction, then the authorization request message will contain all of the following:

- Identity Check Insights
- A Security Level Indicator (SLI) value of 214 in DE 48, subelement 42 (Electronic Commerce Indicators)
- The Directory Server Transaction ID in DE 48, subelement 66 (Authentication Data), subfield 2

Refer to the *Mastercard Identity Check Program Guide* for more information about Identity Check Insights.

Use of EMV 3DS

If an online gambling merchant performs EMV 3DS authentication to comply with this requirement, then the authorization request will contain:

- A valid accountholder authentication value (AAV) in DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF])
- The applicable SLI value in DE 48, subelement 43 (Electronic Commerce Indicators)

Refer to the *Mastercard Identity Check Program Guide* for more information about using Mastercard Identity Check for EMV 3DS authentication.

Compliance

The acquirer of a merchant using MCC 7995 that is not compliant with the current CVC 2 requirement must take immediate action to become compliant. The acquirer of a noncompliant merchant may now use EMV 3DS or send Identity Check Insights to become compliant.

Effective 17 April 2020, the acquirer of any merchants using MCC 7800, 7801, 7802, 7995, or 9406 must provide the CVC 2 value, EMV 3DS, or Identity Check Insights, or a combination of these, in all online gambling transactions. Acquirers should refer to [“AN 2479—Electronic Commerce Security Level Indicators for the Mastercard Identity Check Program”](#) for more information about SLI values arising from the use of Mastercard Identity Check.

Compliance will be monitored, and should volume indicate that a data integrity monitoring program may be necessary to improve compliance, Mastercard will provide details in a future bulletin announcement.

² EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.

Issuer Impact

Effective 17 April 2020, issuers must ensure their authorization systems are prepared to accept authorization request messages for online gambling transactions that may not contain the CVC 2 value, provided either Identity Check Insights are shared or EMV 3DS is used and an AAV is present.

Issuers with authorization management systems and procedures that include rules set to decline non-face-to-face transactions with MCC 7800, 7801, 7802, 7995, or 9406 when the CVC 2 value is not present should modify these rules accordingly.

Issuers should refer to ["AN 2122—Introduction of Mastercard Digital Transaction Insights Service"](#) for more information about a merchant's provision of Identity Check Insights.

Revised Standards

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

Questions?

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