Revised Standards for the Specialty Merchant Registration Program

Mastercard is revising the Standards announced in the article "AN 4654 Revised Standards for the Specialty Merchant Registration Program."

Overview of Revised Standards

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

Effective Date	Changes to Standards in...	Will be Published in...
19 January 2021	*Security Rules and Procedures*	Chapter 6. Fraud Loss Control Standards Chapter 7. Merchant, Submerchant, and ATM Owner Screening and Monitoring Standards Chapter 9. Mastercard Registration Program
19 January 2021	*Mastercard Rules*	Chapter 7. Service Providers Chapter 16. United States Region
19 January 2021	*Transaction Processing Rules*	Chapter 5. Card-Not-Present Transactions

Mastercard will incorporate the revised Standards into a future edition of the manuals. The manuals are available on Mastercard Connect™ via Publications.

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 6. Fraud Loss Control Standards

6.2.1.1 Issuer Authorization Requirements

An Issuer must implement a rules-based authorization strategy with the following parameters:

- Decision matrix for Card validation code (CVC) 1, CVC 2, and CVC 3 validation results
- Limits on single-day and multiple-day Transaction velocity (number of Transactions)
- Limits on single-day and multiple-day monetary spending (value of Transactions)
- ~~Limits~~ Risk-based limits for ~~high-risk~~ identified specialty Merchant Card acceptor business codes (MCCs) and locations on a daily or, if necessary, more frequent basis
- Limits for particular POI entry modes (such as magnetic stripe-read, primary account number [PAN] key-entry, chip-read, Card-Not-Present [CNP])
- Limits for particular country codes
- Decision matrix for expiration date errors
- Decision matrix for Track 1 validation errors
- Decision matrix for geographic anomalies

6.2.1.2 Issuer Fraud Monitoring Requirements

An Issuer must generate daily reports or real-time alerts monitoring both authorization and clearing data. Such reports, if possible, should be generated at the latest on the day following the Transaction(s) for the following parameters:

- Single Transaction exceeding a certain amount (established by the Issuer)
- Multiple Transactions exceeding a certain amount (established by the Issuer)
- PAN key-entry Transactions exceeding a certain amount and/or number (established by the Issuer)
- Transactions taking place at ~~high-risk~~ identified specialty Merchant MCCs and at Merchant locations selected by the Issuer based on risk

6.2.2.1.1 Additional Acquirer Authorization Monitoring Requirements for ~~High-Risk~~ Negative Option Billing Merchants

In addition to the Acquirer authorization monitoring requirements listed in section 6.2.2.1 of this manual, an Acquirer of a ~~high-risk~~ negative option billing

Merchant must monitor authorization Transaction messages to identify when the same Account number appears among different ~~high-risk~~ negative option billing Merchant IDs in the Acquirer's Portfolio within 60 calendar days.

When the Acquirer identifies such an Account, the Acquirer must take reasonable steps to verify that each Transaction conducted by the valid Cardholder with the associated ~~high-risk~~ negative option billing Merchant is a bona fide Transaction.

6.2.2.4 Recommended Additional Acquirer Monitoring

Mastercard recommends that Acquirers additionally monitor the following parameters:

- Mismatch of Merchant name, MCC, Merchant ID, and/or Terminal ID
- Mismatch of e-commerce Merchant Internet Protocol (IP) addresses
- Transactions conducted at ~~high-risk~~ Merchants, Submerchants, and other entities registered in the Specialty Merchant Registration Program (refer to Chapter 9)
- PAN key-entry Transactions exceeding ratio
- Abnormal hours (i.e., outside of normal business hours) or seasons
- Inactive Merchants (i.e., those Merchants that have not yet started to accept Cards as well as those that have ceased to accept Cards)
- Transactions with no approval code
- Transaction decline rate
- Inconsistent authorization and clearing data elements for the same Transactions
- Mastercard *SecureCode* or Identity Check authentication rate
- Fraud volume per Merchant
- Any Merchant exceeding the Acquirer's total Merchant average for fraud by 150 percent or more

6.4.2.1 Authorization Controls

A Group 2 Issuer must implement a rules-based authorization strategy. The strategy must be regularly reviewed and updated as appropriate. Spending limits set by the Issuer within its authorization strategy should be set to have minimum impact on valid Transactions and maximum impact on fraud reduction.

A Group 2 Issuer must include the following parameters in its authorization system:

- A single Transaction exceeding a certain amount (established by the Issuer)
- Multiple Transactions exceeding a certain amount (established by the Issuer)

The Issuer should set specific risk-based limits with respect to:

- ~~High-risk~~ Identified specialty Merchant MCCs and Merchant locations selected by the Issuer based on risk;
- ~~Particular Merchant locations determined to be high-risk~~;
- Particular POS entry modes (for example, magnetic stripe-read, chip-read, or key-entered); and
- Particular country codes.

A Group 2 Issuer should also include rules and parameters based on authorization and clearing data relating to the following:

- Account-generated attacks
- CVC 1, CVC 2, and CVC 3 validation failures
- PIN, ~~Mastercard® *SecureCode*™ token,~~ Account Authentication Value (AAV), Token cryptogram, or ARQC validation failures

Chapter 7. Merchant, Submerchant, and ATM Owner Screening and Monitoring Standards

7.1.1 Required Screening Procedures

The Acquirer of a prospective Merchant or ATM owner, and any Payment Facilitator of the Acquirer with respect to a prospective Submerchant, must ensure that the following screening procedures are performed:

- For a prospective ~~high-risk~~ negative option billing Merchant or Submerchant, identify any entity that provides service for the Merchant or Submerchant that would allow such entity to have access to Account data, and ensure that each such entity is registered with Mastercard as appropriate.

7.4 Additional Requirements for Certain Merchant and Submerchant Categories

~~An Acquirer of a non-face-to-face adult content and services Merchant or Submerchant, non-face-to-face gambling Merchant or Submerchant, non-face-to-face pharmaceutical and tobacco product Merchant or Submerchant, government-owned lottery Merchant or Submerchant, skill games Merchant or~~

~~Submerchant, high-risk cyberlocker Merchant or Submerchant, recreational cannabis Merchant or Submerchant (Canada Region only), high-risk securities Merchant or Submerchant, cryptocurrency Merchant or Submerchant, high-risk negative option billing Merchant or Submerchant, and/or Merchant or Submerchant reported under the Excessive Chargeback Program (ECP)~~ A Customer that acquires or proposes to acquire Transactions submitted by or on behalf of a Merchant, Submerchant, or other entity of a type listed in section 9.1 must comply with the registration and monitoring requirements of the ~~Mastercard~~ Specialty Merchant Registration Program (SMRP) for each such Merchant, ~~or~~ Submerchant, or other entity, as described in Chapter 9.

Chapter 9. ~~Mastercard~~ Specialty Merchant Registration Program

9.1 ~~Mastercard~~ Specialty Merchant Registration Program Overview

Mastercard requires Customers to register the following Merchant types, including Submerchants, and other entities using the Specialty Merchant Registration Program ~~(MRP)~~ system, available via Mastercard Connect™:

- Non-face-to-face adult content and services Merchants—MCCs 5967 and 7841 (refer to section 9.4.1)
- Non–face-to-face gambling Merchants—MCCs 7801, 7802, and 7995 (refer to section 9.4.2)
- For a non-face-to-face gambling Merchant located in the U.S. Region, the Customer must submit the required registration items as described in section 9.4.2 to Mastercard by sending an email message to ~~high_risk_merchant@mastercard.com~~ specialty_merchant_registration@mastercard.com.
- Non–face-to-face pharmaceutical Merchants—MCCs 5122 and 5912 (refer to section 9.4.3)
- Non–face-to-face tobacco product Merchants—MCC 5993 (refer to section 9.4.3)
- Government-owned lottery Merchants (U.S. Region only)—MCC 7800 (refer to section 9.4.4)
- For a government-owned lottery Merchant located in the U.S. Region, the Customer must submit the required registration items as described in section 9.4.4 to Mastercard by sending an email message to ~~high_risk_merchant@mastercard.com~~ specialty_merchant_registration@mastercard.com.
- Government-owned lottery Merchants (specific countries)—MCC 9406 (refer to section 9.4.4)

- Skill games Merchants—MCC 7994 (refer to section 9.4.5)
- For a skill games Merchant located in the U.S. Region, the Customer must submit the required registration items as described in section 9.4.5 to Mastercard by sending an email message to ~~high_risk_merchant@mastercard.com~~ specialty_merchant_registration@mastercard.com.
- High-risk cyberlocker Merchants—MCC 4816 (refer to section 9.4.6)
- Recreational cannabis Merchants (Canada Region only)—regardless of MCC (refer to section 9.4.7)
- High-risk securities Merchants—MCC 6211 (refer to section 9.4.8)
- Cryptocurrency Merchants—MCC 6051 (refer to section 9.4.9)
- ~~High-risk n~~Negative option billing Merchants selling physical products—MCC 5968 (refer to section 9.4.10)
- Merchants reported under the Excessive Chargeback Program (refer to section 8.3)

9.3 General Monitoring Requirements

The monitoring requirements described in this section apply to Customers that acquire non-face-to-face adult content and services Transactions, non–face-to-face gambling Transactions, non–face-to-face pharmaceutical and tobacco product Transactions, government-owned lottery Transactions, skill games Transactions, ~~high-risk~~ certain cyberlocker Transactions, recreational cannabis Transactions (Canada Region only), ~~high-risk~~ certain securities Transactions, cryptocurrency Transactions, ~~high-risk~~ negative option billing Transactions, or Transactions from Merchants reported under the ECP:

9.4.6 High-Risk Cyberlocker Merchants

A non–face-to-face ~~high-risk~~ cyberlocker Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase access directly from a Merchant or Submerchant, or indirectly from an operator or entity that can provide access, to remote digital file storage and sharing services.

Before an Acquirer may process non–face-to-face ~~high-risk~~ cyberlocker Transactions from a Merchant or Submerchant whose contents and services meet one or more of the following criteria, it must register the Merchant or Submerchant, as well as any entities that can provide access to or accept payments on behalf of such Merchant's or Submerchant's contents and services, with Mastercard as described in section 9.2 of this manual~~.~~:

~~In addition, before an Acquirer may process non-face-to-face high-risk cyberlocker Transactions from an entity that can provide access to or accept payments on behalf of a cyberlocker Merchant's or Submerchant's contents and services, it must register the entity, as well as any cyberlocker Merchants for which it provides access, with Mastercard as described in section 9.2 of this manual.~~

~~Any cyberlocker Merchant, Submerchant, or entity that provides access to or accepts payments on behalf of such Merchant's or Submerchant's contents and services that meets one or more of the following criteria must be registered by the Acquirer as a high-risk cyberlocker Merchant, and Mastercard will determine, in its sole discretion, if the Merchant, Submerchant, or entity is a high-risk cyberlocker Merchant:~~

- The cyberlocker Merchant provides rewards, cash payments, or other incentives to uploaders. Some incentives are based on the number of times that the uploader's files are downloaded or streamed by third parties. The Merchant's rewards programs also pay a higher commission for the distribution of file sizes consistent with long-form copyrighted content such as movies and television shows.
- The cyberlocker Merchant provides URL codes to uploaders to facilitate sharing and the incorporation of such links on third-party indexing or linking websites.
- Links to prohibited content stored in the cyberlocker are often found on third-party indexing or linking sites, or by search engine queries.
- Files stored within the cyberlocker Merchant may be purged if they are not accessed or unless the user purchases a premium membership.
- Incentives for premium cyberlocker memberships are based on faster download speed or removing ads, as opposed to storage space. Free access to stored files may otherwise be discouraged by long wait times, bandwidth throttling, download limits, online advertising, or other techniques.
- The cyberlocker Merchant provides a "link checker" that allows users to determine whether a link has been removed, and if so, allows the user to promptly re-upload that content.
- File owners are:
    - Typically anonymous,
    - Not required to provide any identifying information, and

    - Not aware of the identity of those users who have access to or view their files.
- File distribution and sharing are emphasized on the cyberlocker site.
- Storage or transfer of specific copyrighted file types such as movies, videos, or music is promoted on the cyberlocker site.
- Without the purchase of a premium membership, video playback includes frequent display advertisements.

An Acquirer must identify all non–face-to-face ~~high-risk~~ cyberlocker Transactions using MCC 4816 (Computer Network/Information Services) and TCC T.

9.4.8 High-Risk Securities Merchants

A ~~high-risk~~ securities Transaction occurs directly or indirectly in a Card-present or Card-not-present environment when a consumer uses an Account to purchase, sell, or broker a financial instrument, including but not limited to derivatives (for example: forwards, futures, options, and swaps).

Before an Acquirer may process ~~high-risk~~ securities Transactions from a Merchant, Submerchant, or other entity that facilitates one or more of the following activities, the Acquirer must register the Merchant, Submerchant, or other entity with Mastercard as described in section 9.2 of this manual~~.~~:

~~Any securities Merchant, Submerchant, or entity that facilitates one or more of the following activities must be registered by the Acquirer as a high-risk securities Merchant, and Mastercard will determine, in its sole discretion, if the Merchant, Submerchant, or entity is a high-risk securities Merchant:~~

• Binary options trading

• Contracts for difference (CFD)

• Foreign exchange (Forex) currency options trading

• Cryptocurrency options trading

• Initial coin offerings (ICOs)

An Acquirer must identify all face-to-face high-risk securities Transactions using MCC 6211 (Securities—Brokers/Dealers) and TCC R (for face-to-face Transactions) or TCC T (for non-face-to-face Transactions).

~~An Acquirer must identify all non-face-to-face high-risk securities Transactions using MCC 6211 and TCC T.~~

To register a Merchant, Submerchant, or other entity, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing

the following items to Mastercard upon request as part of the registration process (herein, all references to a Merchant also apply to a Submerchant or other entity):

1. **Evidence of legal authority**. The Acquirer must obtain from the Merchant:

– a copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority in each country where ~~the Merchant's~~ high-risk trading activity as described in this section will occur or be offered to Cardholders, that expressly authorizes the Merchant to engage in such trading activity;

– a copy of the Merchant's registration, where required under applicable law, with a licensed exchange or licensed trading platform; and

– any law applicable to the Merchant that permits such high-risk trading activity.

The Acquirer must provide an updated license(s) to Mastercard prior to expiration. If an Acquirer is unable to obtain an updated license, then the Acquirer must cease processing applicable high-risk securities Transactions from such Merchant until the Acquirer is able to provide an updated license to Mastercard.

2. **Legal opinion**. The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a reputable law firm located in each country where high-risk trading activity as described in this section will occur or be offered to Cardholders. The legal opinion must:

– identify all relevant trading laws and other laws applicable to the Merchant;

– identify all relevant trading laws and other laws applicable to Cardholders that may transact with the Merchant; and

– demonstrate that the Merchant's and Cardholders' trading activities comply at all times with any laws identified above.

The legal opinion must be acceptable to Mastercard. Further, the Acquirer shall ensure that:

– the Merchant properly maintains its lawful status in any jurisdiction where such Merchant engages in high-risk trading activities as described in this section; and

– any relevant permits remain unexpired.

3. **Effective controls**. The Acquirer must obtain certification from a qualified independent third party demonstrating that the Merchant's systems for operating its high-risk securities business:

– include effective age and location verification; and

– are reasonably designed to ensure that the Merchant's high-risk securities business will remain within legal limits (including in connection with cross-border Transactions).

4. Notification of changes. The Acquirer must certify that the Acquirer will notify Mastercard of any changes to the information that the Acquirer has provided to Mastercard, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to Mastercard (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.

5. Acceptance of responsibilities. The Acquirer must specifically affirm that it will not submit restricted Transactions from the Merchant for authorization. If a Merchant's non-face-to-face high-risk trading activities are regulated as gambling in any jurisdiction, then the Acquirer must register such Merchant as a non-face-to-face gambling Merchant with Mastercard as described in section 9.2 and section 9.4.2 of this manual.

9.4.10 ~~High-Risk~~ Negative Option Billing Merchants Selling Physical Products

A non-face-to-face ~~high-risk~~ negative option billing Transaction for the sale of physical products occurs in a Card-not-present environment when a consumer uses an Account to purchase a subscription service to automatically receive one or more physical products (such as cosmetics, health-care products, or vitamins) on a recurring basis (such as weekly, monthly, semi-annually, or annually).

The subscription service may be initiated by an agreement between the consumer and the Merchant or Submerchant whereby the consumer (Cardholder) receives from the Merchant or Submerchant a sample of the product (either complimentary or at a nominal price) for a trial period. The sample may be larger, equal to, or smaller than the product provided by the Merchant or Submerchant during the subscription period. For the purposes of this section 9.4.10, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the physical product such as its quality or usefulness to determine whether the Cardholder wants to either:

• Purchase the product on a one-time basis or recurring basis; or

• Return the product (if possible) to the ~~high-risk~~ negative option billing Merchant.

After the trial period has expired, a non-face-to-face ~~high-risk~~ negative option billing Transaction may occur ~~on a recurring basis~~ each time that the product is shipped to the Cardholder, using Account information provided by the

Cardholder to the Merchant or Submerchant ~~each time that the product is shipped to the Cardholder~~ upon the Cardholder's initiation of the subscription. The non-face-to-face ~~high-risk~~ negative option billing Transactions continue to occur on a recurring basis until either:

• The Cardholder takes action to terminate the agreement with the Merchant or Submerchant (for example, notifying the Merchant or Submerchant to cancel the subscription);

• The Merchant or Submerchant terminates the agreement; or

• The subscription expires.

Before an Acquirer may process non-face-to-face ~~high-risk~~ negative option billing Transactions involving physical products, including magazine and newspaper subscriptions, from a Merchant or Submerchant, the Acquirer must register the Merchant or Submerchant, as well as any entities that provide service to such Merchant or Submerchant that allow access to Account data, with Mastercard as described in section 9.2 of this manual.

An Acquirer must use MCC 5968 (Direct Marketing—Continuity/Subscription Merchants) and TCC T to identify all non-face-to-face ~~high-risk~~ negative option billing Transactions.

Revised Standards for the *Mastercard Rules*

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

Chapter 7. Service Providers

7.6.7 Staged Digital Wallet Operator Requirements

NOTE: Modifications to certain provisions of this Rule appear in the "Canada Region," ~~and~~ "Europe Region," and "United States Region" chapters.

Chapter 16. United States Region

7.6.7 Staged Digital Wallet Operator Requirements

In the U.S. Region, a provision of the Rule on this subject is modified as follows:

G. MCC 6540 must not be used for a funding stage Transaction if such funds may subsequently be used for the purchase of any products or services for which the Acquirer must register the entity conducting the sale as described in Chapter 9 of the *Security Rules and Procedures*; in such event, the MCC that best describes the nature of the purchase must be used, and the funds must be

segregated and made available for use by the consumer solely for the designated purpose.

Revised Standards for the *Transaction Processing Rules*

Mastercard will revise the *Transaction Processing Rules* to include these Standards. Additions are underlined and deletions are indicated with a ~~strikethrough~~.

Chapter 5. Card-Not-Present Transactions

5.1.1 E-commerce Transactions—Acquirer and Merchant Requirements

10. For a physical product or a sample of the physical product provided to a Cardholder by a ~~high-risk~~ negative option billing Merchant for a trial period, the trial period begins on the date that the Cardholder receives the product.

For purposes of this Rule 5.1.1, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the product such as its quality or usefulness to determine whether the Cardholder wants to either:

– Purchase the product on a one-time basis or recurring basis; or

– Return the product (if possible) to the ~~high-risk~~ negative option billing Merchant.

11. If the Merchant is a ~~high-risk~~ negative option billing Merchant, then the Merchant must provide a direct link to an online cancellation procedure for recurring payment Transactions on the website on which the Cardholder initiated an agreement with the Merchant to bill the Cardholder on a recurring basis for one or more physical products provided by the Merchant through the Merchant's website.

5.4 Recurring Payment Transactions

5.4.1 ~~Recurring Payment Transactions for High-Risk~~ Negative Option Billing Merchants

The following Standards apply to recurring payment Transactions associated with a ~~high-risk~~ negative option billing Merchant:

1. The Acquirer must process all subsequent recurring payment Transactions using the same Merchant ID in DE 42 (Card Acceptor ID Code) and Merchant name in DE 43, subfield 1 (Card Acceptor Name) as the Acquirer used for the initial payment Transaction.

2. After the trial period for a physical product has expired, the ~~high-risk~~ negative option billing Merchant must provide the following information to the Cardholder and receive the Cardholder's explicit consent in relation to this information before the Merchant may submit an authorization request for the initial recurring payment Transaction:

– The Transaction amount

– The payment date of the Transaction

NOTE: After the Cardholder has provided consent, the Merchant may not change this date; however, a later payment date may be offered by the Merchant prior to consent, if the authorization request results in a declined response from the Issuer due to insufficient funds in the Cardholder's Account.

– The Merchant name as it will appear on the Cardholder's statement

– Instructions for terminating the recurring payment Transaction cycle (for example, canceling the subscription service) at the Cardholder's discretion. For purposes of this Rule 5.4.1, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the product, such as its quality or usefulness to determine whether the Cardholder wants to either:

– Purchase the product on a one-time basis or recurring basis; or

– Return the product (if possible) to the ~~high-risk~~ negative option billing Merchant.

3. Each time that the Merchant receives an approved authorization request, the Merchant must provide the Cardholder with a Transaction information document (TID) through an e-mail message or other electronic communication method (such as an SMS "text message") including instructions for terminating the recurring payment Transaction cycle (such as canceling the subscription service). If the Merchant provides the Cardholder with a TID after a declined authorization request, the TID must state the reason for the decline response.

4. The Merchant must provide the Cardholder with written confirmation in either hard copy or electronic format when either or both of the following events occur:

– The Cardholder's trial period expires

– The recurring payment Transaction cycle has been terminated by either the Merchant or the Cardholder

For more information about ~~high-risk~~ negative option billing Merchants, refer to section 9.4.10 of the *Security Rules and Procedures* manual.