Accepting the Mastercard® Biometric Card

Mastercard is committed to helping acquirers learn more about the Biometric Card and how to handle it without any new software. As more financial institutions decide to issue cards with embedded biometric sensors, you may notice an increasing number of customers using such cards in your merchant locations. This pamphlet will help you to be prepared to accept these cards and to understand how they can be used.

The Mastercard Biometric Card provides a simple and secure way for cardholders to authenticate their identity for in-store purchases using their fingerprint, as an alternative to using PIN or signature. It is a chip card that can authenticate both contact and contactless transactions biometrically. An embedded sensor authenticates the cardholder's identity through an enrolled fingerprint using power drawn from the terminal or NFC technology, so there is no battery needed in the card.

Like digital wallets, the Biometric Card can be used for paying above the terminal's contactless limit* without the need for a PIN or signature. The card can do a biometric "capture and compare" entirely on the card, similar to digital wallets. The biometric data is stored securely as a digital template on the cards; this is never shared externally. The results of the biometric match are shared with the issuer as part of the authorization request.

The card is the same thickness as other cards and is designed to work biometrically at Mastercard EMV terminals worldwide, with no impact on terminals or acquirer software.

Merchant Point-of-Sale Experience

STEP 1

Merchant enters purchase details then submits to terminal, just as they do today.

Reminder: Contactless-enabled Biometric Cards can be used for payments above the usual contactless limit.

STEP 2

A cardholder places their thumb on the sensor built into the card then taps the card or inserts it into the EMV terminal.

A new digital image of the cardholder's thumbprint is created on the card, using power from the terminal.

STEP 3

The new digital thumbprint image is compared against the stored digital template on the card.

The biometric match results are sent to the EMV chip, and the transaction data is sent to the issuer in the authorization request.

If matching is not possible, the terminal will ask for another authentication method, such as PIN or signature, based on the issuer's preference.

STEP 4

The issuer receives the chip data indicating whether the biometric match was successful or whether it failed. The issuer uses this data to help make its approval decision.

Merchant receives authorization response.

*THRESHOLD IS DEPENDENT ON MERCHANT COUNTRY AND ACQUIRER POS SETUP

Processing points for acquirers and payment processors

Ordinarily, in a regular PIN or signature transaction, tag 9F34 (Cardholder Verification Method (CVM) Results) would indicate which cardholder verification method has been used. **However, for a Biometric Card the CVM results cannot be solely relied upon**. This is because when CVM is carried out successfully on the Biometric Card, the **Application Interchange Profile (AIP)** indicates that cardholder verification is not supported by setting the "cardholder verification is supported" bit to zero. When this bit is set to zero, the terminal will skip CVM processing altogether.

The Cardholder Verification Results (CVR) in Issuer Application Data (tag 9F10) contains the result of the biometric match to be passed to the issuer. Therefore, the CVR appears only in the issuer application data and is relevant only to the issuer.

Acquirers can confirm that biometric authentication has been used by checking that the AIP B1b5 of tag82 in DE 55 is set to zero. The AIP is a mandatory field that the acquirer should already be checking. **It is in the acquirer's interest to identify successful biometric matching. If the transaction has been duly approved, the issuer will be liable for any related transaction losses.**

Acquirer liability

The introduction of the Biometric Card does not change any dispute rights.

The chargeback liability remains with the issuer if the biometric match is successful. If the biometric match is not successful, then the transaction will be processed using the highest priority CVM commonly supported by both the card and terminal, which may be PIN or signature. In that situation, standard chargeback rules will apply. Please refer to the Chargeback Guide regarding the chip and chip & PIN liability shifts.

Terminal requirements

The Biometric Card requires no changes to acquirer or merchant hardware or software, as it is compatible with any EMV-enabled terminal that has satisfactorily completed the Mastercard Terminal Integration Process (M-TIP) and is operating on current valid specifications from Mastercard and EMVCo. A Biometric Card can also be used on a contactless terminal that has been updated for Apple Pay or Google Pay acceptance.

MORE INFORMATION

For more background information, please refer to Mastercard's previous publications AN2151 and AN1353 on Mastercard Connect®, which covers changes to chargeback and transaction processing rules.