ADVANCING PAYMENT SECURITY

MASTERCARD CONTACTLESS SECURITY OVERVIEW

ABOUT MASTERCARD CONTACTLESS PAYMENT

First introduced in 2005, MasterCard contactless technology enables consumers to make fast, convenient, and secure payments by simply tapping their contactless-enabled card, mobile phone, or other form factor* anywhere MasterCard contactless is accepted. MasterCard contactless payment devices contain a chip and use radio frequency technology to wirelessly transmit data to the merchant's specially equipped contactless-enabled POS terminals. The consumer initiates the transaction with a tap instead of swiping a magnetic stripe or inserting a chip card at the POS.

MasterCard contactless transactions are processed through the same financial payments network that processes billions of MasterCard magnetic stripe and chip card transactions each year. They use the same security techniques as traditional chip cards where each transaction uses encryption to protect the payment data. This, along with other safeguards built into the technology, ensure that contactless payment devices cannot be easily compromised. MasterCard places a strong and consistent emphasis on security through compliance with product specifications and other MasterCard requirements to safeguard consumers, merchants, and other payment system participants.

During the contactless transaction process, a dynamic cryptogram is generated by the contactless payment device. The cryptographic data is then validated by either the contactless reader or by the issuer of the payment device, depending on if the transaction is to be approved offline or online. A successful validation is essential to ensure that only transactions from authentic payment devices are accepted.

The security measures are designed to meet the following security requirements:

» Protect against fraud

» Prevent card data reuse

» Maintain consumer confidentiality

*Contactless payment devices encompasses, card, mobile phone and other form factors.

SECURITY IS AT THE FOUNDATION OF CONTACTLESS TECHNOLOGY

MasterCard considers security to be the foundation of its contactless technology. Transactions are authenticated online to the issuer or offline by the point-of-sale (POS) device.

ONLINE AUTHENTICATION

A contactless Magstripe mode transaction authorization includes a unique one-time cryptogram, referred to as a Dynamic CVC3 (dCVC3) that is generated by the contactless payment device based on data from the POS terminal and data stored on the payment device.

A contactless M/Chip mode transaction that is to be authenticated online by the issuer (determined by the issuer parameters on the contactless payment device and POS parameters) will provide an Authorization Request Cryptogram that is generated by the payment device based on data plus cryptographic keys stored on the payment device.

OFFLINE AUTHENTICATION

A contactless M/Chip mode payment device that supports offline authorization is required to support Combined Data Authentication (CDA), a public key cryptogram authentication method which provides the highest level of assurance that the contactless payment device and payment cryptogram are genuine. This type of transaction allows secure payments to be conducted in locations where going online is not possible or is cost prohibitive such as transit systems, street parking meters, or onboard a ferry. In this case, authentication of the payment data is performed by the contactless reader using a MasterCard certification authority public key loading in the POS.

For offline authorizations, the contactless payment device will provide a Transaction Certificate that is generated by the payment device based on data from the POS terminal and data stored on the payment device.

The use of CDA for local authentication of the contactless payment device by the terminal is usually also performed if the transaction goes online.

SECURE THE FUTURE OF PAYMENTS

SECURITY

Fraudulent reuse of transaction data is prevented by requiring a unique cryptogram for each authorization. Created in real-time, the cryptogram is used by the issuer to authenticate a transaction. In the event of the data being replayed, its reuse can be detected in a subsequent transaction by checking the cryptogram, allowing the issuer to take appropriate action.

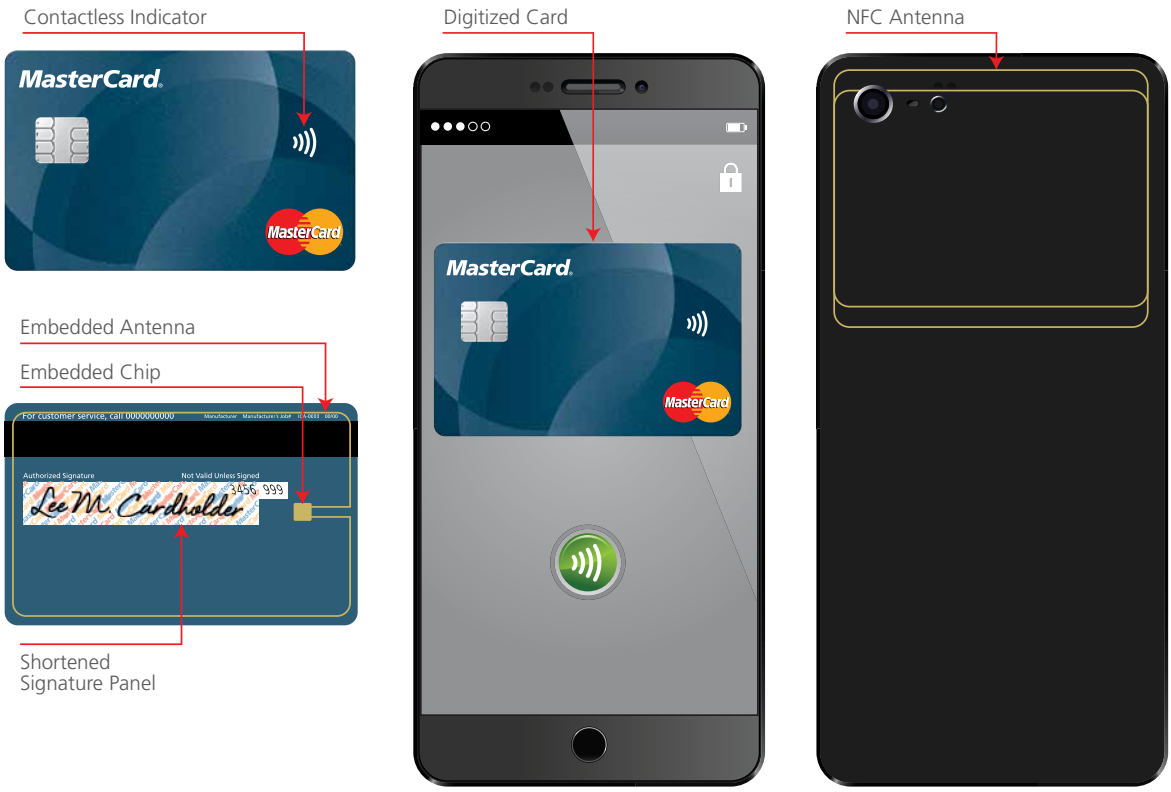
- For protection against card-not-present fraud, **the Card Validation Code (CVC2)**, is not present in the data on the chip.
- On a MasterCard contactless-enabled mobile phone, the CVC2 information may be available but cannot be accessed from the mobile phone using a contactless reader.
- In the authorization request of each transaction, MasterCard requires identification of the transaction **POS Entry Mode** as contactless for MasterCard contactless transactions. Also, the issuer uses the POS Entry Mode in conjunction with the dynamically generated card or mobile cryptogram to verify if the transaction has been properly introduced via a contactless POS. This protects against data "sniffed" contactlessly being used to create a counterfeit magnetic stripe card for use at a swipe POS device. In addition an Unpredictable Number is used to provide freshness to the transaction data.
- Subsets of contactless-enabled payment devices that cannot be dipped or updated over the air such as tags or key fob must always go online to the issuer for authentication and authorization since additional checks are conducted.

PROTECTION

- The processing of contactless payments does not require the use of the consumer name in the transaction. Therefore, MasterCard requires that the consumer's name must not be included in the transaction data.
- MasterCard contactless transactions above a certain locally established transaction value may require the consumer to perform cardholder verification in addition to tapping the contactless payment device. These include PIN or signature at the POS terminal, or for devices such as mobile, **On-Device Cardholder Verification** (ODCV) methods which include PIN or an approved biometric verified on the payment device.
- Contactless payment devices supporting M/Chip mode transactions have the ability to allow issuers to control offline transaction spending for payment values below the cardholder verification method limit by using offline counters and accumulators in order to prevent uncontrolled use of lost or stolen cards. Exceeding the counter or accumulator limit may lead to a request for a card to perform a contact transaction or mobile device to require ODCV.
- MasterCard **Limitation of Liability of Cardholders for Unauthorized Use** applies to all MasterCard cards issued in Asia/Pacific, Canada, Europe, South Asia/Middle East Africa, and the United States.*

CONTROL

- The consumer does not have to hand over their payment device to a clerk during a contactless transaction.
- Transactions are conducted only when the **payment device is between 0–4cm (centimeters) of the terminal** and if the merchant has initiated the transaction.



*Conditions and exceptions apply. See the MasterCard Rules for more details.

ALL STAKEHOLDERS IN THE PAYMENT CHAIN HELP TO LIMIT FRAUD

Security in the payment system depends on all stakeholders in the value chain working together to adopt best practices and implement required solutions.

ISSUERS

- Use only type-approved MasterCard payment applications and chips.
- Successfully complete the required testing and follow other MasterCard recommended security safeguards when issuing and maintaining MasterCard and Maestro branded payment devices.
- Use a contactless specific PAN-range for payment devices to enhance risk management capabilities.

ACQUIRER

- Deploy only type-approved POS devices.
- Successfully complete required MasterCard testing.

CONSUMER

- Proactively monitor their accounts and report to their issuer any suspicious transactions, as well as alert their issuer without undue delay if their payment device is lost or stolen.
- When provided with the functionality by the issuer, consumers are also encouraged to proactively manage their accounts by setting up real-time alerts using MasterCard In Control.™

Additional Resources

We don't expect you to know everything there is to know about contactless. But we do want you to know how to find the answers.

mastercard.com/contactless
contactless@mastercard.com

These are your go-to resources for all things contactless. Connect to country-specific contactless sites and find implementation information and marketing support specific to merchants, issuers, and acquirers.

mastercardconnect.com
mastercardbrandcenter.com

Cardholders can use mastercard.com/contactless to access the contactless Merchant Locator tool which can help them find contactless-accepting merchants around the world—online or through an app for mobile.

For more information, contact your MasterCard customer representative or email contactless@mastercard.com. To view Chip Publications, visit mastercardconnect.com