

# CONTACTLESS TOOLKIT

## FOR ISSUERS



**1.9 billion** AN ESTIMATED 1.9 BILLION CARDS WILL BE USED FOR CONTACTLESS PAYMENTS GLOBALLY IN 2018.\*

We live in a rapidly evolving digital world, a world in which consumers are always connected. Increased connectivity is changing consumer expectations. They want faster, more secure payments and better overall service. Issuers can meet these changing expectations by offering MasterCard contactless payments.

**PURPOSE OF THIS TOOLKIT**

This *Contactless Toolkit for Issuers* is designed to help issuers successfully implement a MasterCard Contactless program and integrate best practices.

**Table of Contents**

Welcome to Contactless ..... 1

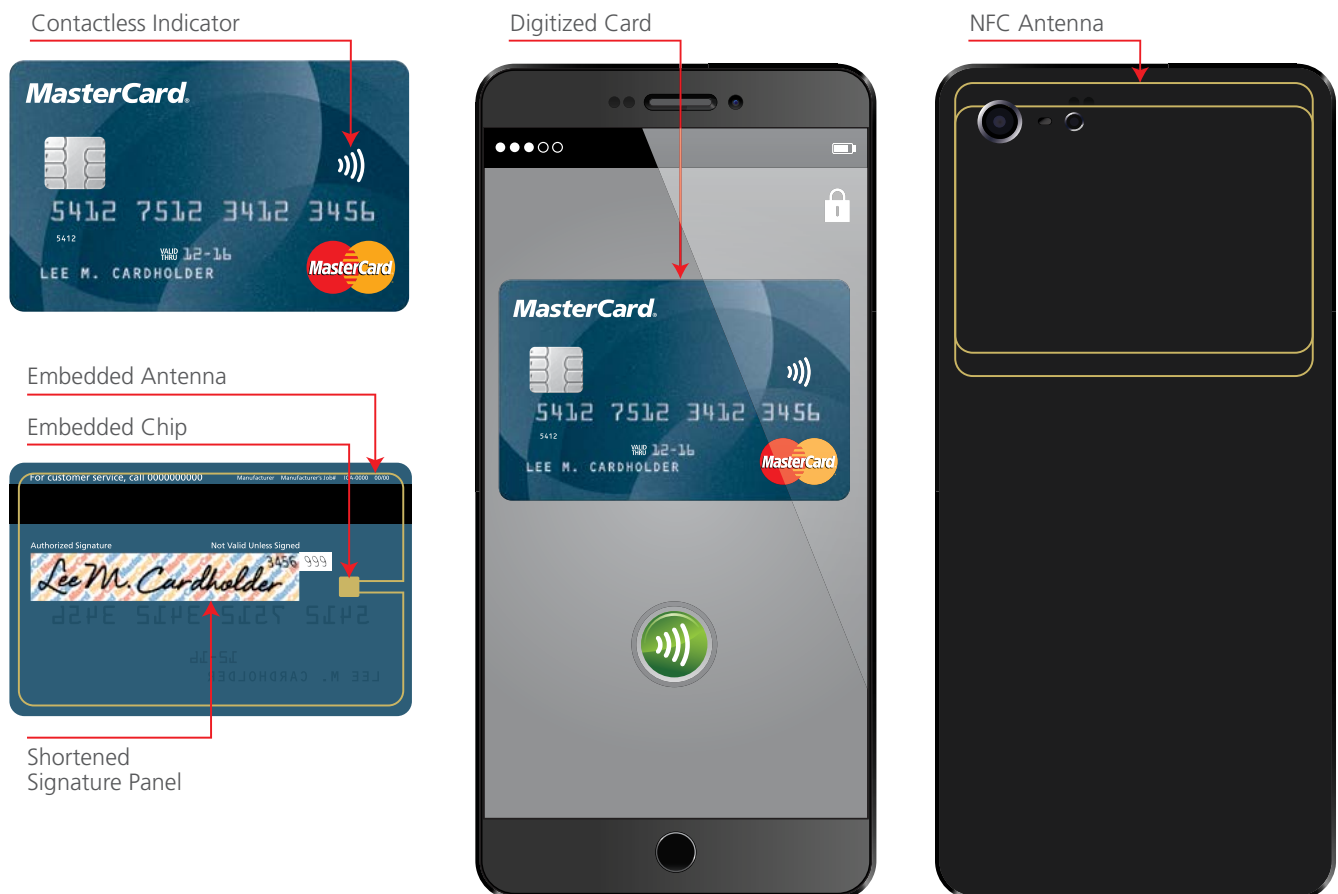
How it Works..... 3

FAQs..... 5

Four Steps to Implementation ..... 8

## Welcome to Contactless

Making payments has never been easier, thanks to contactless payments. All the cardholder needs to do is tap their contactless-enabled card, mobile phone, sticker, key fob or other form factor<sup>1</sup> on a contactless-enabled reader or terminal.<sup>2</sup> Within a fraction of a second, they'll receive payment confirmation, and be on their way.



1 The term "payment device" refers to a plastic card, mobile phone or any other form factor used for payment, and "cardholder" refers to the user of the payment device.

2 The term "reader" refers to the equipment which the consumer taps, whether integrated into the POS terminal or connected to it.

### 3+ MILLION

MasterCard or Maestro contactless cards or devices can be used at over 3 million merchant locations in 68 countries around the world.

MasterCard Data Warehouse, 1Q2015

## WHAT IS CONTACTLESS?

Contactless is a payment method that gives your cardholders the convenience of making payments without swiping or dipping a payment card.

Instead, the cardholder simply taps their contactless-enabled payment device onto a contactless-enabled reader.

The chip and antenna in the payment device securely transmit payment details wirelessly to a contactless reader, either integrated within or connected to a merchant's point-of-sale (POS) system. For lower value payments, the cardholder will normally receive payment confirmation immediately and can be on their way. The transaction details are subsequently cleared through the same acceptance network used for traditional payment card transactions. In some markets the low value and high value transactions will be send online for approval by the associated issuer.

Contactless cards look similar to standard MasterCard and Maestro cards. But embedded inside them is a computer chip that stores and processes the payment account data and a connected antenna that typically runs around the perimeter of the card. Similar chip and Near Field Communication (NFC) technology powers contactless payments made by mobile phones and other form factors.

Contactless capability is denoted by the universal **Contactless Indicator** (see below) which is present on all contactless cards and form factors or should be displayed on the screen of contactless mobile devices.

A **Contactless Symbol** is present on all contactless readers to indicate compliance with EMV Contactless Communication Protocol, and the Contactless Symbol must be used to indicate the "read area" on the reader where the payment device should be tapped.

Any payment device with a Contactless Indicator will work on any reader with a Contactless Symbol. This global interoperable acceptance is an important part of the MasterCard contactless payment proposition



Contactless Indicator (Payment Device)



Contactless Symbol (Reader)

## How it Works

### CARDHOLDER VERIFICATION

Traditional payments normally require some Cardholder Verification Method (CVM) such as PIN or signature. For low-value contactless payments below the “Contactless CVM limit,” no CVM is required—the consumer can simply tap & go.™ Note that the Contactless CVM limit varies from country to country.

Cardholder verification is required for contactless card transactions above the CVM limit (e.g., by online PIN using the merchant PIN pad or signature). The merchant is liable for contactless transactions above the CVM limit that have no cardholder verification.

A new form of CVM called Consumer Device Cardholder Verification (CDCV) is available with mobile contactless devices. In this case the consumer enters a PIN (or biometric) on the device. Two versions are supported:

- » **Early CDCV.** The consumer provides the verification before the tap (typically while waiting in the line or queue).
- » **Two-Tap.** The consumer taps their device onto the reader to start the transaction, moves their phone away for CDCV when prompted, and taps again to complete the transaction.

CDCV can also support biometric verification, if the mobile device is fitted with a fingerprint reader for example, and other verification methods may be supported in the future like pattern and vein recognition.

CDCV is designed to work with new versions of the MasterCard contactless terminal, known as “Contactless Reader v3.0” or “MCL 3.0.” These are being rolled out globally and MasterCard has mandated that all new contactless terminals are MCL 3.0 compliant.

For contactless transactions below the CVM limit, a receipt is not required unless the consumer requests it. For transactions above the limit, a receipt must always be provided.



**70%**

The number of active contactless accounts worldwide increased 70% year-over-year in 2014.

MasterCard Key Metrics, 1Q2015

**CONTACTLESS MODES**

Contactless payments may be Magstripe mode or EMV mode.

In countries which have not yet migrated to EMV chip, the majority of contactless transactions will be Magstripe mode. Contactless magstripe cards contain a chip as well which generates the same data as that generated by swiping the card, with the addition of a cryptogram, known as the dynamic CVC3.<sup>3</sup> In order to authenticate this cryptogram, all Magstripe mode contactless transactions should be authorized online by the issuer.

In countries which have migrated to EMV chip, the majority of contactless transactions will be EMV mode. In this case the chip supports MasterCard's M/Chip payment application which is capable of approving contactless transactions offline, without reference to the issuer. Such off-line authorization is faster than online authorization and is therefore normally employed, especially in environments with high throughput or less connectivity. Issuers can also set their M/Chip Dual Interface cards to require only online authorization. For added security M/Chip makes use of counters for risk management. An issuer can set these counters to require a contact rather than a contactless transaction whenever the number or cumulative amount of contactless transactions has reached certain limits.

Contactless transactions initiated by mobile devices may optionally support other risk management features:

- » "No-CDCV Counters" (sometimes referred to as "Lost & Stolen Counters") which periodically force CDCV after a certain number or amount of No-CDCV transactions.<sup>4</sup>
- » Payment Activation ("Say When I Want to Pay") which allows the consumer to switch on mobile payment only when they want to use it, and switch it off the rest of the time.
- » Amount Acknowledgement ("Confirm Amount I Want to Pay") which is the process of obtaining a positive action by the consumer, typically a single press or CDCV, to confirm that they approve the transaction amount.

**OFFLINE AUTHENTICATION**

A contactless EMV 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.

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

<sup>3</sup> CVC: Card Verification Code

<sup>4</sup> Feature limited to EMV mode mobile devices

## Frequently Asked Questions

### How will issuing MasterCard Contactless benefit my business?

Contactless acceptance is proven to bring many benefits for issuers and their cardholders, including:

#### Issuers:

- » Incremental spend—consumer not limited to cash on hand
- » Incremental transactions—results from increased usage
- » Expected increases in swiped/dipped transactions
- » Replacement of cash purchases now paid with contactless-enabled cards and devices
- » Provides an infrastructure for mobile payment capabilities
- » Opens up new merchant acceptance opportunities such as mass transit and tollways

#### Cardholders:

- » Enables secure payment with mobile phone
- » Provides a faster, simple, and safe way to pay for purchases
- » Offers greater convenience, eliminating need to restrict spend to cash on hand
- » Allows cardholder to maintain control during purchases

### What are the latest consumer insights on contactless performance?

Since the original contactless trials in 2003, we have continued to see strong usage and an increase in user adoption. Contactless is successfully displacing cash in environments where cash was traditionally the preferred payment method—where the average ticket is low. In fact, approximately 88% of contactless transactions are under \$50.<sup>5</sup> Plus, contactless-enabled accounts increase and maintain higher average spend per account than non-contactless-enabled accounts: 26% YOY net lift in spend among contactless credit accounts and 39% among contactless debit accounts.<sup>6</sup>

### What types of merchants can benefit the most from contactless acceptance?

Contactless acceptance is an excellent choice for any merchant, especially in environments where speed and convenience are valued and cash is currently the dominant payment method, such as supermarkets, quickservice restaurants (QSRs), drive-thrus, convenience stores, vending machines, tollbooths, taxis, parking venues, fuel pumps and public transport. Contactless payment is recognized as the only realistic option for ticketless mass transit systems.

### How safe are these transactions?

MasterCard has put in place a number of measures which mean that contactless payments are highly secure:

- » Every contactless transaction is protected by a unique cryptogram which proves that the payment device is genuine and means the transaction cannot be fraudulently replayed
- » Below the CVM Limit all EMV mode transactions are either authorized offline subject to offline card authentication (CDA) & risk management, or are authorized online with a dynamic cryptogram. All Magstripe mode transactions are authorized online.
- » The processing of contactless payments does not require the use of the cardholder name in the transaction. Therefore, MasterCard requires that the consumer's name must not be included in the transaction data.
- » Above the CVM limit the consumer will be prompted to use PIN, signature or CDCV.

**39%**

Contactless-enabled accounts increase and maintain higher average spend per account than non-contactless-enabled accounts: 26% YOY net lift in spend among contactless credit accounts and 39% among contactless debit accounts.

MasterCard Data Warehouse, FY2013 and FY2014

<sup>5</sup> MasterCard Data Warehouse, 4Q2014

<sup>6</sup> MasterCard Data Warehouse, FY2013 and FY2014

**\$18.82**

In 2014, global MasterCard contactless average ticket size was \$18.82. Approximately 77% and 93% of transactions were for purchases under \$25 and \$50, respectively—a sign that contactless is displacing cash.

MasterCard Key Metrics, 1Q2015

- » The POS Entry Mode field in all contactless transactions is set as “contactless” to verify that transactions properly originate at a contactless terminal. 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.
- » For protection against card-not-present fraud, the Card Validation Code (CVC2), is not present in the data on the chip.
- » Some M-Chip cards will allow the contactless interface to be disabled and enabled after the first contact chip transaction.
- » With mobile devices, a variety of additional security measures are possible, and issuers may also choose to use “tokens” instead of “real” card account numbers (PANs) in a process called “tokenization.”
- » The cardholder keeps possession of the payment device throughout a contactless payment transaction.
- » Transactions are conducted only if the merchant has initiated the transaction and usually when the device is about 2 cm from the reader.

**Does contactless acceptance change the payment guarantee for the merchant?**

If a contactless payment is authorized, online or offline, the merchant still receives a payment guarantee, even for transactions below the CVM limit with no cardholder verification.

**How does pricing work—do contactless transactions cost more or less than traditional credit and debit transactions?**

Contactless interchange rates for issuers depend not just on the technology but also on a range of other factors, including the region where the transaction takes place, whether it is cross-border, and the underlying existing payment product.

**What are the costs involved?**

For most issuers, the costs of implementing contactless are modest. Dual interface cards cost very little more than cards without contactless capability. And although provisioning mobile payment devices require system changes, issuers do not bear the costs of issuing plastic.

**What type of technology is used for contactless?**

In keeping with overall MasterCard strategy to create globally interoperable payment solutions, contactless payments are compliant with all relevant industry standards including EMV.

**How are contactless readers identified?**

To use a contactless payment device, consumers must look for the universal Contactless Symbol as described above.

**How is issuing mobile payment device different from cards?**

Although mobile payment transactions are processed very similarly to contactless card transactions, the process of provisioning and managing mobile payment devices is in some respects quite different. In this toolkit, these differences are highlighted in boxes, starting with a summary of key features below.





## MOBILE NFC PAYMENTS

### SUMMARY OF KEY FEATURES

- » The issuer needs to work with a new ecosystem of mobile payment stakeholders.
- » Mobile devices usually feature a digital wallet from which the cardholder selects one of a number of “cards” via a user interface.
- » Payment applications are usually personalized, loaded and activated “over-the-air” (OTA) in a mobile provisioning process.
- » In addition to payment transactions, the issuer will need to process a variety of management transactions.
- » Mobile devices may also be used for remote m-commerce payments using MasterCard’s Digital Secure Remote Payments (DSRP) solution.
- » MasterCard supports two types of mobile contactless payment solution. With **MasterCard M/Chip Mobile** solution, the payment application and sensitive payment credentials are stored on a Secure Element (SE) or Trusted Environment on the handset or in the SIM. With **MasterCard Cloud Based Payments (MCBP)** solution, the payment credentials are stored securely on the device using a process known as Host Card Emulation (HCE) and the cryptogram is securely generated in the cloud. While all the features listed above still apply to both types of solution, issuers will be impacted in different ways depending on which solution is adopted.

These mobile payment features and the way they are supported by the two MasterCard solutions are covered in more detail in boxes in the sections which follow. For a full explanation, please refer to:

- » *M/Chip Mobile Issuer Implementation Guide* (for MasterCard’s SE solution)
- » *MasterCard Cloud Based Payments (MCBP) Issuer Implementation Guide* (for MasterCard’s HCE solution)

For issuers wishing to implement mobile payment functionality rapidly, with minimal disruption to current operations, MasterCard offers an on-behalf MasterCard Digital Enablement Service (MDES). For details, please refer to *MasterCard Digital Enablement Service, Issuer Implementation Guide*.

Implementing mobile payments brings new challenges but it also brings significant new opportunities. In the longer term, it is expected that mobile payments will enable a range of exciting new value added features and hybrid payment opportunities such as sophisticated loyalty and coupon schemes, GPS alerts, and scanning QR coupons in-store, or from a PC.

## Four Steps to Implementation

### 1. PRE-IMPLEMENTATION PLANNING

Successful initiatives don't just happen, they are planned. MasterCard recommend taking the time to develop a comprehensive contactless implementation project plan. Gather the right resources and stakeholders to discuss the project in its entirety to help ensure a successful implementation.

#### DECISION MAKING

Pre-issuance planning starts with a decision making phase. Decision making addresses business requirements and the technical means that you use to achieve those requirements. These decisions directly affect how you will implement adding contactless to your M/Chip or Magstripe issuance and therefore affect the planning required. Key decisions which you will need to make include the following:

- » Contactless payment is likely to be the first step in a larger global adoption of innovative payment technologies like Mobile NFC which could provide innovative issuers with significant business opportunities in the future.
- » Make sure you understand any rules and practices which apply to your local market such as CVM limits, offline authorization policies, EMV migration status, and so on. MasterCard will help but it may also be worth talking to a national payments authority if one is available.
- » Plan how to maximize the benefits of your move to contactless, through first class staff training in particular, but also through effective communications with cardholders and possible rewards and other incentive schemes.
- » Consider the best strategy for coordinating contactless implementation with existing issuing lifecycles. In the US, the migration to EMV is likely to be a good opportunity for a more comprehensive issuing strategy.

#### PROJECT PLANNING

Having made key decisions, you are ready to create a project plan. Like any important initiative, contactless implementation requires good project management and this involves appointing all stakeholders from the outset, and above all, agreeing on a plan which addresses all key deliverables.

#### WORKING WITH MASTERCARD

After formalizing your business decisions and creating your own project plan, you need to contact your regional MasterCard representative to initiate a Contactless Migration Project. MasterCard will assign a MasterCard project manager, who will, with your help, produce a Customer Implementation Plan detailing all key deliverables pertaining to the MasterCard approval process.

MasterCard can also assist you with the following:

- » Contactless strategy support and decision making.
- » Workshops covering business, technical, operational and security needs.

#### CHANGE COMMUNICATION

Throughout the project, and particularly during the implementation phase, you need to communicate to staff and cardholders the changes that you will introduce with contactless, and encourage them to leverage the tap & go™ message.

With any new program launch, the goal is to drive incremental usage through added consumer value. Communications should be specific and engaging—explain how this will benefit the cardholder. Additionally, employees are often a main contact point for your customers and they need to not only be aware of the product or feature capabilities, but also be an advocate of its use.

MasterCard has marketing templates, design guidelines and FAQs, available to help you develop your communications and marketing messages as well as cardholder-specific materials. Having an appropriate communications plan will contribute to the overall success of your program. Please refer to the MasterCard Marketing Center for the necessary details.

## LICENSING

Vendors are required to enter into a license agreement with MasterCard before developing and selling payment devices. All payment devices, and readers used for performing contactless transactions must be approved and licensed by MasterCard prior to their use. Detailed information about the type approval process can be found by linking to the Chip Information Center at [mastercardconnect.com](http://mastercardconnect.com)

Issuers must start a project with the relevant MasterCard project team in order to define and complete various approval steps that are required, including Host Testing, Card Personalization Validation (CPV), Key Management Services and Live Environment Validation.

## MOBILE NFC PAYMENTS



### PLANNING YOUR MOBILE PAYMENTS ECOSYSTEM

Implementing a mobile payment program involves working with a new “mobile ecosystem” of stakeholders such as network operators, handset manufacturers, Trusted Service Managers (TSMs) and wallet providers in addition to traditional acquirers and merchants.

MasterCard’s M/Chip Mobile solution has been designed to be highly flexible and robust in order to accommodate this diversity, with multiple options to meet the needs of all stakeholders. Nevertheless M/Chip Mobile implementation is challenging and requires careful planning and execution to be successful.

With MasterCard’s MCBP solution, issuers are no longer so reliant on the network operator which owns the SIM, but other processes are then required to emulate the security of the SE. This too will require careful planning.

## BEST PRACTICE GUIDELINES



Work closely with MasterCard to make sure you fully understand local market conditions and rules.



Treat contactless implementation as just part of a larger issuing strategy, taking into account the opportunities of mobile payments.



If planning to implement mobile payments from the outset, then work closely with MasterCard and other mobile ecosystem partners.

## 2. PAYMENT DEVICE DESIGN AND PERSONALIZATION

Although the same payment device design and personalization principles apply to both contactless cards, devices and mobile devices, the details are somewhat different. The sections below deal specifically with “cards” (including form factors such as fobs and stickers). Special considerations applying to mobile devices are highlighted in the *Mobile Payments: Designing and Provisioning Mobile Payment Devices* section.

### DESIGN CARDS AND OBTAIN CARD DESIGN APPROVAL

Redesign your cards to carry the Contactless Indicator and obtain card design approval.

### SELECT A CARD VENDOR/PRODUCT

Select a card vendor which offers card products that meets your business requirements. The vendor product must meet and maintain compliance with other MasterCard requirements, specifically Compliance Assessment and Security Testing (CAST) and Card Quality Management (CQM). The card product itself must meet and maintain Card Functional Approval (CFA). The device selected also needs a valid non-expired LOA for the product (MasterCard, Maestro) they intend to issue. Refer to the Chip Information Center at [mastercardconnect.com](http://mastercardconnect.com) for the list of approved contactless products. Alternatively, you can choose to develop your own product, under license, based on the contactless specifications and MasterCard requirements. Your product will need to obtain approval and this process is normally extremely technical and will impact your time to market.

### DISCUSS MIGRATION WITH YOUR PERSONALIZATION BUREAU

If you use a personalization bureau, discuss with them your plans to add contactless to EMV or Magstripe mode cards and how they can help you achieve this.

### UPDATE CARD MANAGEMENT SYSTEMS

You need to make changes, if necessary, to your card management system, such as preparing and sending additional data for personalization.

### CONDUCT CARD PERSONALIZATION VALIDATION

Your contactless-enabled devices must obtain Card Personalization Validation (CPV) to ensure that the personalization parameters in them meet all MasterCard requirements. MasterCard recommends that you use standard personalization profiles to quickly accomplish CPV. Using non-standard personalization profiles will result in a longer and costlier CPV due to the need for more extensive testing and analysis. MasterCard further recommends that you test your cards before submitting them for CPV. This may be achieved by requesting assistance from a test laboratory or by using one of the available qualified test tools



## MOBILE NFC PAYMENTS

### DESIGNING AND PROVISIONING MOBILE PAYMENT DEVICES

**Designing the User Interface.** With mobile payments, a “wallet” or user interface application allows the cardholder to interact with the payment application by, for example, choosing a card to pay with, entering a PIN on the handset, responding to on-screen instructions or reading transaction details. The wallet may also support over-the-air (OTA) communication, for application loading, updating and management—in other words, all the actions which would be carried out via script messaging with a contact chip card, and more.

MasterCard mobile products will work with a wide range of wallets, from simple, single card applications to sophisticated, multi-card wallets. **MasterPass™ by MasterCard** is an example of the latter. MasterCard supports wallet developers with a User Interface Software Development Kit (UI SDK).

**Application loading and personalization.** A key benefit of mobile payments is the ability to instantly deliver a personalized payment application OTA to the cardholder. This raises a number of new issues that must be carefully managed, including: the sign-up process (Identification and Verification); ensuring handsets are compatible and identified; ensuring the Secure Element (if applicable) is compatible and identified; and reliability of loading. MasterCard provides support in all these areas.

**Type Approval.** To ensure integrity and interoperability, all elements of an M/Chip Mobile implementation are required to be Type Approved by MasterCard. This extends not just to the traditional elements of a card payment product, but also to new components of the ecosystem such as the Secure Element, User Interface, Contactless Front End, Handset and Trusted Service Manager(s). Similar type approval requirements apply to MCBP solutions.

### BEST PRACTICE GUIDELINES



Use approved vendors and make sure products meet all MasterCard approval criteria.



For mobile payment devices, pay particular attention to the design of the user interface or wallet, working with specialized vendors in most cases.



Application loading and personalization of mobile payment solutions will be a new type of operation for most issuers and should be managed carefully with mobile ecosystem partners.

### 3. SYSTEM CHANGES

#### MAGSTRIPE MODE VS. EMV MODE

The changes required for your systems will depend on whether you are issuing Magstripe mode devices or EMV mode devices (mobile devices are generally EMV mode). If you are in a region which has not yet migrated to EMV chip and you wish to issue EMV contactless devices, then this is probably a good opportunity to migrate all payment products to EMV.

#### AUTHORIZATION SYSTEM CHANGES

If you are issuing Magstripe mode payment devices then your system must support dynamic CVC3 processing to authenticate the dynamic cryptogram in the authorization message.

If you are issuing EMV mode payment devices then your system must support Authorization Request Cryptogram (ARQC) authentication processing and Chip data validation in the authorization message. You could also support offline risk management, which involves using offline risk parameters and counters within the chip application to require an online authorization whenever the number or cumulative amount of offline transactions has reached certain limits. While an online authorization is performed, the issuer can determine if the counters are then set to zero using the EMV response message.

#### CLEARING SYSTEM CHANGES

New values have been identified for certain existing Data Elements in the MasterCard-defined authorization and clearing records for contactless transactions. Your systems must be able to identify and check the "POS Entry Mode" and "POS Terminal Input Capabilities" and Chip Data Elements and take appropriate actions.

#### NETWORK INTERFACE VALIDATION

You or your issuer processor will need to obtain Network Interface Validation certification with MasterCard to ensure that both authorization and clearing system changes are compliant with MasterCard requirements.



## MOBILE NFC PAYMENTS

### ADDITIONAL SYSTEM CHANGES

If you are provisioning mobile payment devices, further system changes are required, including:

- » Application loading and personalization systems
- » Other mobile risk management systems (i.e., Payment Activation, Amount Acknowledgement and No-CDCV counters)
- » CDCV management (Early CDCV or Two-Tap, with, optionally, a distinct PIN for mobile use only)
- » OTA management functionality to support functions such as confirmations, balance reporting, transaction history, unblocking PINs, and optionally offline authorization management.
- » Optionally, support for remote payments using MasterCard's Digital Remote Secure Payment solution.
- » Optionally, the capability to provide a richer transaction with additional payments-related propositions such as vouchers, location-based services, or support for alternative checkout experiences such as transactions initiated with the use of QR codes.

For more details, please refer to *MIChip Mobile* and *MICBP Issuer Implementation Guides*.

### BEST PRACTICE GUIDELINES



Don't skimp on testing. Effort spent on this step will save time and money during later deployment.



Allow plenty of time. Card schemes will be dealing with multiple entities so schedule generous testing slots well in advance.



If you are issuing EMV mode payment devices for the first time, consider full migration to EMV chip (depending on market condition).



If you are provisioning mobile contactless devices, take advantage of enhanced functionality to deliver an outstanding new proposition.

## 4. LIVE SYSTEM MIGRATION AND ROLLOUT

### DEVELOP DEPLOYMENT SCHEDULE

Your deployment schedule should take the following considerations into account:

- » **Need for a Pilot**—Consider whether you need a pilot project before full rollout. Contactless technology is now fairly mature; for issuers in regions where contactless payments are already established a pilot is probably not required. For issuers that are pioneering contactless payment issuance in their local markets, or for mobile device issuance, a pilot is recommended.
- » **Segmentation**—Select which cardholder segments you wish to provide with contactless payment capability, and in what order. Identify and target specific consumer segments that have been shown to be early adopters. This applies particularly for mobile device programs.
- » **Timing**—Optimize the timing of your pilot and rollout.
- » **Testing**—Identify how testing will occur throughout the network, host, card pilot and live rollout process.
- » **Training**—Identify the training tools, FAQ and processes that will be provided to your customer-facing staff.

### PRODUCTION SETUP

Allow for the time needed to move from development to production:

- » Switching network connections from development to production.
- » Enabling BINs for contactless-enabled cards.
- » Ensuring that personalization uses live keys instead of test keys.
- » Allow for the MasterCard On-Behalf-Of service setup (e.g., Stand In parameters).

### CONDUCT END-TO-END DEMONSTRATION

Carry out a successful End-to-End Demonstration (ETED) to validate that you are able to issue live payment devices that can be accepted and operate in the correct manner in an issuer or processor production environment via the MasterCard network. ETED is strongly recommended for mobile deployments.

### EMPLOYEE TRAINING

Specific training must be incorporated into any ongoing employee training program. Guiding principles include:

- » Educate employees at least four weeks before issuance.
- » Train employees immediately after announcing a launch.
- » Generate excitement with all communications.
- » Consider an employee promotion or sweepstakes during the rollout phase. Cardholder-facing employees should be knowledgeable about contactless payment and act as an advocate of its use.

The objective of training is to:

- » Give cardholder-facing employees product and benefit information so they can answer questions.
- » Highlight typical cardholder questions and give employees model answers that could help in the sales process.
- » Encourage employees to promote the card and highlight usage opportunities.



## CONDUCT A PILOT (IF REQUIRED)

A pilot will help ensure that issuer employees are adequately trained, software and hardware are working correctly, and your operation is set up correctly before you move to wider deployment. Here are the key steps:

- » Perform staff training
- » Select pilot cardholders
- » Issue payment devices
- » Observe and record problems, solutions, and opportunities.
- » Adjust processes as necessary and integrate best practices before initiating a full rollout

## IMPLEMENT AND MONITOR ROLLOUT

After a successful pilot, you'll be able to confidently roll out your issuing program. To help ensure that your cardholders have a positive contactless experience, continuously monitor and actively address any issues that arise during and after implementation.

## DEPLOY PAYMENT DEVICES TO CARDHOLDERS

Deploy contactless-enabled cards and form factors using an appropriate deployment strategy.

## CARDHOLDER COMMUNICATION

Effective cardholder education and communication is essential to the success of a contactless launch. In order to get cardholders to activate and use the card or device right away, issuers need to:

- » Highlight the benefits of contactless payment
- » Explain how it works
- » Reassure your customers about potential security concerns
- » Provide guidance on where contactless payment is accepted (MasterCard provides merchant locator application in most regions)
- » Market to your customers in a consistent, frequent and multi-phased manner.

Issuers should use multiple channels for communications, including:

- » Effective staff training
- » Inserts with card mailers
- » National and regional media campaigns
- » Marketing initiatives at selected merchants
- » Joint programs with network operators or handset manufacturers for mobile payment products

## USAGE CAMPAIGNS

Getting contactless-enabled portfolio customers to activate and establish the tapping habit can be done effectively through usage incentives like a tap & get promotion.

## PERFORMANCE MONITORING

Ongoing performance monitoring is necessary in order to effectively evaluate the performance of the contactless functionality on any portfolio, and to design programs that further promote usage. Issuers need to ensure that they are able to identify their contactless-enabled customers and determine when they swipe/dip vs. tap their card/device. Important elements of performance monitoring include:

- » Clearly identify metrics to measure
- » Define test period
- » Identify target group and split into test and control segments
- » Evaluate impact

### MASTERCARD PROJECT CLOSURE AND POST-IMPLEMENTATION MONITORING

Following a successful ETED, MasterCard Customer and Product Delivery will close the implemented project on its side and will start post-implementation monitoring for 30 days to watch for any problems that may occur as your live contactless transactions begin.



### MOBILE NFC PAYMENTS

#### ADDITIONAL ROLLOUT CONSIDERATIONS

The same guidelines apply to the rollout of a mobile payment rollout as to a contactless card rollout, but certain aspects are particularly important and require close cooperation between an issuer and its partners in the mobile payment ecosystem:

- » **Deployment of payment devices.** For mobile payments, application loading and activation will normally be carried out Over-the-Air (OTA) following a secure cardholder registration process. This will be unfamiliar to most of your customers. Therefore, the process needs to be simple, streamlined and planned carefully.
- » **Consumer marketing.** Once again, consumers will be unfamiliar with mobile payment so issuers will need to make a particular effort to explain how it works, why it is secure and the particular functionality of the product (CDCV, Early CDCV vs Two-Tap, user interface design, management functions, etc). The use of visuals and checkout illustrations is recommended.
- » **Ongoing management communication.** OTA capability means issuers have additional opportunities to communicate with cardholders via the mobile device, delivering educational, marketing and support messages.
- » **Added value features.** As mobile payment continues to evolve, issuers will be able to leverage the enhanced functionality of this new technology with a wide range of added value features.

For more details, please refer to the *MiChip Mobile* and *MCBP Issuer Implementation Guides*.

#### BEST PRACTICE GUIDELINES



Make sure employees are fully trained, engaged with the rollout, and encourage your customers to tap and go.™



Focus on making sure your customers are aware of the contactless payment option and have a positive experience.



Don't be afraid to fine-tune deployment based on lessons learned.



Work with mobile ecosystem partners to address the particular implementation challenges of a new mobile device rollout.



BANK LOGO



**CHOOSING THE JUICEST APPLE: 3 MINUTES**



**PAYING FOR THE APPLE: FASTER THAN ONE BITE**



**MasterCard & Maestro contactless. Tap & Go™**  
 It is quick and easy. Just tap the terminal with your card, no need to dip it.  
 For purchases over 25 EUR you have to enter your pin for added security.\*

\*In some markets, e.g. UK or France, for purchases above the local limit you need to dip your card and enter your PIN.



BANK LOGO

**I MANAGED TO PAY FOR THE PETROL BEFORE MY KIDS EVEN NOTICED ALL THE SWEETS IN THE SHOP.**

**Time to switch to MasterCard Contactless.**



**MasterCard & Maestro contactless. Tap & Go™**  
 It is quick and easy. Just tap the terminal with your card, no need to dip it.  
 For purchases over 25 EUR you have to enter your pin for added security.\*

\*In some markets, e.g. UK or France, for purchases above the local limit you need to dip your card and enter your PIN.

Consumer Marketing in Europe: Posters focus on the availability and benefits of using contactless-enabled cards and devices.

## Video

Fast Payments at  
Globus Supermarkets  
[bit.ly/Globusvideo](http://bit.ly/Globusvideo)

Just Tap & Go™ with  
MasterCard Contactless  
[bit.ly/ConsumerSecurityVideo](http://bit.ly/ConsumerSecurityVideo)

Cashless Pioneers:  
Transport for London  
[bit.ly/TflvideoMA](http://bit.ly/TflvideoMA)

## 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](http://mastercard.com/contactless)  
[mastercardconnect.com](http://mastercardconnect.com)  
[mastercardbrandcenter.com](http://mastercardbrandcenter.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.

Cardholders can use [mastercard.com/contactless](http://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 relationship manager.**