

"Offering a simple, more secure online shopping experience with Mastercard® Identity Check™"

Mastercard Identity Check Playbook for Acquirers and Merchants

2019



Table of Contents

- 1. Introduction**
- 2. Overview: PSD2, SCA and Mastercard® Identity Check™**
- 3. Mastercard's Authentication Strategy**
- 4. SCA Exemptions**
- 5. Your Communication Toolkit**
Key Messages, Visuals, Design Templates, Website Content, FAQs, User Journeys, Consumer Information Video, Branding Guidelines
- 6. What's next**

Appendix

Back to Basics, What is Mastercard® Identity Check™, How we help





1. Introduction



Introduction

If you are working in the payments industry you cannot fail to be aware that 2019 brings the final deadline to comply with the Payment Services Directive 2 Regulatory Technical Standards (PSD2 RTS). Since the RTS were published in early 2018, the payment community has been actively engaged in understanding, clarifying and planning for the measures to be implemented to ensure compliance by the 14th September 2019.

The introduction of Strong Customer Authentication (SCA) is a major step forward in the move to a more secure payments eco-system, but if poorly executed it has the potential to have a significant detrimental impact upon the consumer experience. If not yet done, we strongly recommend to make yourself familiar with the situation and gain insight to decide on how your business will handle SCA and what user experience you will provide to your customers.

Why you should read this guide?

With the PSD2 RTS having such significant ramifications for the payments industry it is not surprising that typing related key words into Google will generate thousands and thousands of results. Whether you are looking for opinions, guidelines, white papers or even the standards themselves there is plenty from which to choose. So is there really a need for yet another piece on SCA?

Here are three reasons why reading this guide will benefit your business.

The first: We share this information in the belief that by working together we can ensure a smoother transition for all stakeholders to a safer and more secure payments eco-system. However, this guidance is provided for general information purposes only and does not constitute legal advice. It is not intended as a substitute for taking appropriate legal advice and such advice should be taken before acting on any of the topics covered.

Given that questions re. SCA continue to be submitted and new EBA (European Banking Authority) responses published, any paper can inevitably be no more than a reflection of what was known at a point in time. So with points still being clarified, it is important that you should regularly consult your own legal advisors for any updates and their interpretation of the regulations.

(...)

Why you should read this guide?

(...)

The second is to share Mastercard's perspective on the implementation of this Directive. Through our extensive work to understand the ramifications of PSD2 RTS and our conversations with our customers we have gathered insight that has enabled us to develop guidelines and recommendations that we believe will help to ensure that in fulfilling the requirements of the PSD2 RTS we deliver a frictionless and compliant experience.

And finally, and perhaps the point which lends some urgency to this issue, is that our research indicates that many European online Merchants are still not aware of the SCA requirements. If we are to avoid a deluge of declines for non-compliant transactions once the deadline arrives, it is essential that all participants in the payment ecosystem are not only aware of the requirement for SCA, but have a plan to implement it by the deadline. In publishing this toolkit we aim to provide useful insight and messaging that can inform conversations with your customers and support the efficient delivery of SCA.

The purpose of the consumer communication toolkit



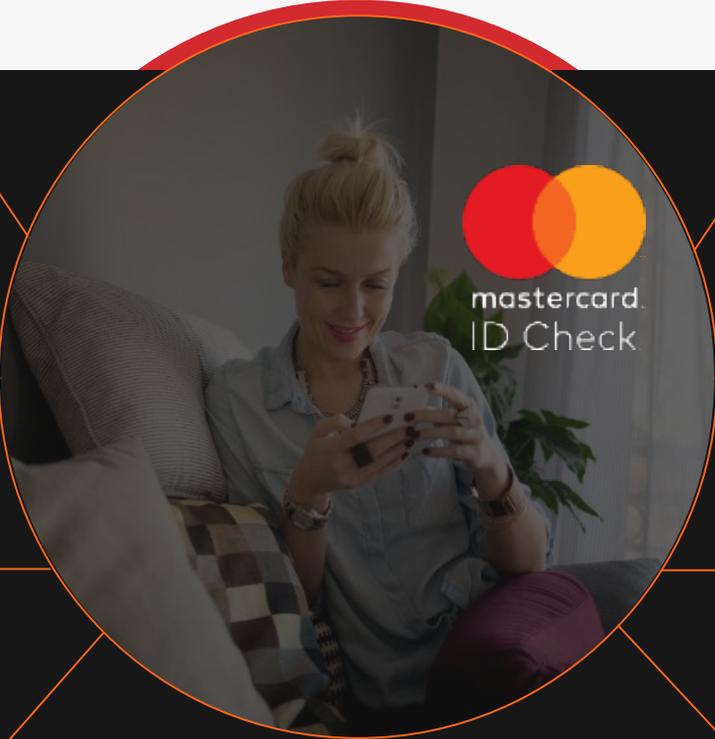
This communication toolkit has been designed to help you effectively communicate and promote Mastercard® Identity Check™ to your customers and guide them through the transition.

It provides you with central assets for all the key communication touchpoints you might use to inform your customers about the transition, guide them through the process and enable them to seamlessly use their Mastercard® card for electronic payments after September 14, 2019.

It also contains selected background information about the regulatory changes, including the many benefits you enjoy as a Merchant/Acquirer/PSP.

Supporting you to educate your customers through your own communication channels

Mastercard Identity Check toolkit overview



1 Key Messages

2 Key Visuals

3 Design Templates

4 Website Content

5 FAQs / Help pages

6 User Journeys

7 Information Video

8 Mastercard Brand



2. Landscape



Current landscape

As countries around the globe move to EMV chip, organized crime looks for a new path to exploit card fraud, with digital commerce as their preferred channel. Today, card-not-present (CNP) fraud accounts for as much as 73% of all fraud¹, with more transactions migrating to CNP channels every day. This migration represents a key challenge for Merchants and Issuers trying to prevent fraud without disrupting their customers' purchasing experience.

For many in the industry, false decline rates are more troubling than fraud losses. False declines occur when a good customer's transaction is mistakenly declined by the Issuer's or Merchant's fraud models. The CNP channels are disproportionately impacted by false declines, with the average decline rate for a CNP transaction hovering around 15% to 20%, versus 2% to 3% for card-present transactions².

In 1999 when the industry introduced 3-D Secure (3DS), the objective was to reduce fraud and improve customer authentication during CNP transactions. And while the protocol helped recreate the security of a physical payment and shifted liability for fraud losses away from businesses, it clearly had some gaps, including failing to address the issue of false declines as evidenced above.

Other challenges:

- It increased customer friction
- It provided a poor customer experience with an inconsistent user interface
- It was limited to browser-based transactions

But this year with the global launch of the new version EMV[®] 3DS it is expected to solve all the gaps that the previous protocol had while improving the security of digital commerce.

PSD2 RTS: What is it ?

PSD2 RTS stands for the EU Payment Services Directive 2 Regulatory Technical Standards that were published in early 2018

PSD2 RTS require that from the 14th September 2019, Strong Customer Authentication (SCA) must be used for all remote electronic transactions, including e-commerce, unless an exemption applies (please see below for details). Merchants must therefore send authentication requests using the EMV® 3-D Secure (EMV 3DS) protocol or support alternative technical SCA solutions to avoid that Issuers decline ecommerce transactions. In recent surveys around 20% of large Issuers have indicated that post-RTS, non- EMV 3DS transactions will be declined to avoid non-compliance.

The RTS will apply in the 31 countries which make the European Economic Area or EEA (which includes the 28 EU countries plus Norway, Iceland and Liechtenstein).



The RTS aims to reduce fraud by mandating SCA for electronic payments, including card payments from browsers or in-app payments, on all types of devices. It details the requirements of when to apply SCA as well as the exemptions from SCA

EMV[®] 3DS: What is it?

EMV 3DS is the evolution of the current authentication interface (3DS 1.0) into an industry standard that:



Lets more transaction and consumer data be exchanged (e.g. device data, shipping and billing address), allowing the Issuer to apply SCA exemptions and enhance decisioning.



Supports new payment needs, such as in-app and mobile payments.



Supports additional use cases, such as:

- Credential-on-file (COF): no need for customers to enter card details into Merchant/retailer's website or app for each purchase as card is pre-registered.
- Wallets, e.g. Google, Samsung Wallets.
- Tokenisation: a token replaces the real card number being stored, avoiding compromise when hacked.



Mastercard® Identity Check™: The new Mastercard programme supporting Merchants and the RTS

- ✓ Mastercard Identity Check is the new programme and brand for Mastercard authentications based on the new EMV® 3DS standard.
- ✓ It replaces the former SecureCode® programme (which could ultimately still serve as fallback) and the previous 3-D Secure version.
- ✓ Identity Check requires minimum performance levels for authorisation approvals, fraud and abandonments to be met by Issuers.



European Issuers are required to start offering their Cardholders biometric authentication solutions via smart phones, which have the lowest abandonment and fraud rates, therefore resulting in the highest sales conversion rates.

An opportunity for Merchants: EMV® 3DS and Mastercard® Identity Check™

With EMV 3DS and Identity Check, e-commerce Merchants will be able to achieve the same performance levels as physical store Merchants (using Chip & PIN, as measured on the Mastercard network*):

- on average 10 percentage points higher approval rates
- up to 50% reduced fraud rates
- around 50% lower abandonment rates

These results can be achieved by letting Issuers apply SCA to every online purchase and providing them with sufficient data to apply exemptions from SCA, so transactions can be completed with minimal friction. Online Merchants must support EMV 3DS authentication requests or alternative technical SCA solutions that comply with PSD2 RTS and Mastercard rules as of April-December 2019 (depending on country).

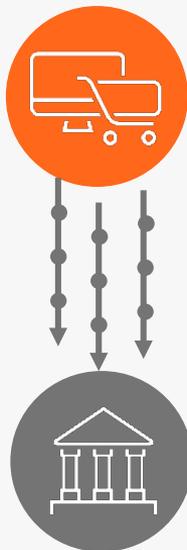


EMV® 3-D Secure and Mastercard® Identity Check™ come with a list of new benefits for Merchants

EMV 3DS addresses a number of key limitations of the previous 3-D Secure 1 protocol. It is projected to become one of the strongest solutions in the fight against card-not-present (CNP) fraud - without sacrificing the shopping experience.

Key changes include:

- **More robust security** to fight fraudulent online transactions – through strong customer authentication, such as biometric and token-based authentication, instead of static passwords
- **Compatibility with mobile devices**, to reflect the growing m-Commerce trend, including in-app payments
- **Improved Risk Based Authentication (RBA)** through the exchange of significantly more contextual data related to the purchase than possible with 3DS 1
- **A frictionless user experience** to reduce shopping cart abandonment



With EMV 3DS Merchants can share more contextual data with Issuers – which creates a win-win-win situation

- ✓ Having more data to analyze with each transaction enables Issuers to apply a **more accurate risk assessment** and approve most transactions based on risk based authentication (RBA).
- ✓ Getting most transactions approved based on RBA empowers Merchants to offer a **frictionless checkout experience** for the Cardholder without compromising on strong security
- ✓ Enjoying a frictionless checkout experience reduces cart abandonment and increases **consumer satisfaction and loyalty**

SCA exemptions - overview: When and how are these applied?

The RTS allows Payment Service Providers (e.g. Issuers and Acquirers) to apply the following exemptions for remote transactions:

For low value payment transactions equal to or below €30, however even low value payments require SCA for every sixth transaction, or if the cumulative amount is higher than €100 since the last SCA.

When applying transaction risk analysis (TRA) of payment transactions for which the amount and fraud level do not exceed pre-defined limits as per the RTS (e.g. a payment initiated by a Cardholder that has not generated any fraud scenarios before, from the same device as used during previous purchase, for an amount up to €100 and where the Acquirer fraud levels do not exceed 13 basis points).

For recurring payment transactions of the same amount and payee. SCA is required when setting up the initial recurring payment agreement including a correct setting of the amount, expiration and frequency of the recurrence. Subsequent recurring transactions shall include reference to the initial agreement.

For transactions to Merchants that were listed by Cardholders as trusted beneficiaries (so-called 'white-list' exemption). SCA is required for the creation or amendment of the white-list of trusted beneficiaries. Only Issuers may apply this exemption. Unless the Acquirer applies an SCA exemption, the Issuer is liable for fraud if an authorization was approved, provided that the Merchant sent an authentication request for the transaction.

Out of Scope of the PSD2 RTS on SCA

For Merchant Initiated Transactions (MIT). As confirmed by the EBA, MITs are out of scope under the following conditions: the transaction is triggered by the Merchant and the Cardholder is off-session or the transaction is triggered by the Merchant as it could not have triggered during Cardholder checkout.

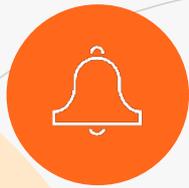
SCA exemptions: When and how are these applied?

Authentications using EMV® 3DS are the recommended method for the Merchant to advise the Issuer about the exemption being applied by the Acquirer. Such authentications typically won't require a Cardholder challenge (e.g. could not lead to an abandonment) but they will allow the Issuer to control the risk which increases the approval rate.

To comply with PSD2 RTS, as of 14 September 2019 Acquirers must ensure that their Merchants use 3DS authentication requests or alternative technical SCA solutions unless an Acquirer exemption applies. Authorization without authentication is allowed if an Acquirer exemption is applied as per PSD2 RTS, however, such transactions usually have lower approval rates.



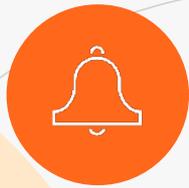
What are the top actions Merchants need to take?



1. Merchants must select and deploy their PSP (Payment Service Provider)/3DS Server that implements and operates the authentication interface on their behalf through EMV® 3DS and 3DS 1.0 (as fallback when Issuer does not support EMV 3DS).
2. Merchants must prepare themselves to capture incremental transaction and Cardholder data (e.g. billing and shipping address, e-mail, mobile phone number or device ID) and send them to the PSP which may require the coding for a new API (Application Programming Interface) or similar provided by the PSP. Merchants shall ensure that their terms and conditions reflect the collection and sharing of the consumer data (e.g. in the privacy notice) as required for example by the General Data Protection Regulation (GDPR).
3. Merchants need to implement an authentication policy, aligned with their PSP and Acquirer, in support of the RTS and its exemptions, specifically to the adoption of TRA exemptions and corresponding fraud levels that apply.
4. Merchants must ask their Acquirer(s) to enroll them for EMV 3DS with the card schemes.
5. Merchants need to make changes to their websites in support of EMV 3DS, the RTS and Mastercard® Identity Check™. One of these changes is the adoption of the Identity Check programme logo.
6. Should a Merchant request an Acquirer SCA exemption without an authentication request, and the transaction is declined by the Issuer (especially for reasons other than financial or technical declines), then a mechanism should be in place that automatically sends an EMV 3DS authentication requesting a challenge and, if approved, followed with another authorisation. Similarly, if an Issuer does not yet support EMV 3DS authentications then a Merchant should use the current 3DS version 1.0.2 as a fallback.

(...)

What are the top actions Merchants need to take?



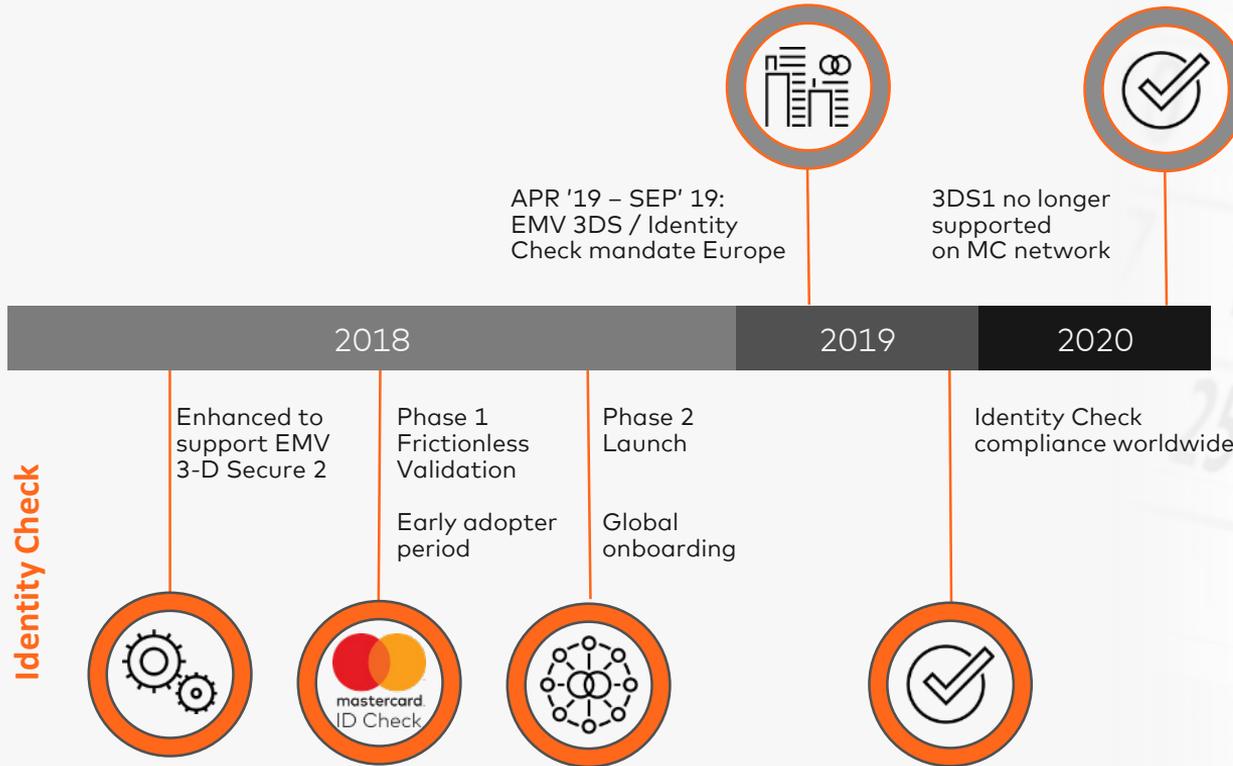
(...)

8. Merchants must ensure name consistency and uniqueness. Best performance of authentication and authorization processes is obtained when Merchant name is consistent. Merchants may benefit optimally from white-list exemptions when they can be recognised with one unique name.
9. Merchants are recommended to always send authentication requests, especially with Issuers that decline authorizations without prior authentication.
10. Integrate EMV® 3DS features to offer an optimal end-consumer experience, by revamping the authentication part of the Merchant app in native User Interface (UI) to offer the same look and feel as the Merchant app.
11. Merchants have to apply SCA to the first recurring payment. In order to increase the approval rates, it is recommended that for each subsequent payment an EMV 3DS authentication request is sent to the Issuer with a reference to the initial SCA to avoid that the Cardholder is asked to authenticate.
12. In case of recurring payments for variable amounts or payments where the final amount is not known, the Merchant should clearly communicate and explain to the end consumer the reasons why the authenticated amount could be different than the final authorization amount. Additional amounts should anyway be within reasonable customer expectations.

Migrating to Identity Check™ / EMV® 3-D Secure

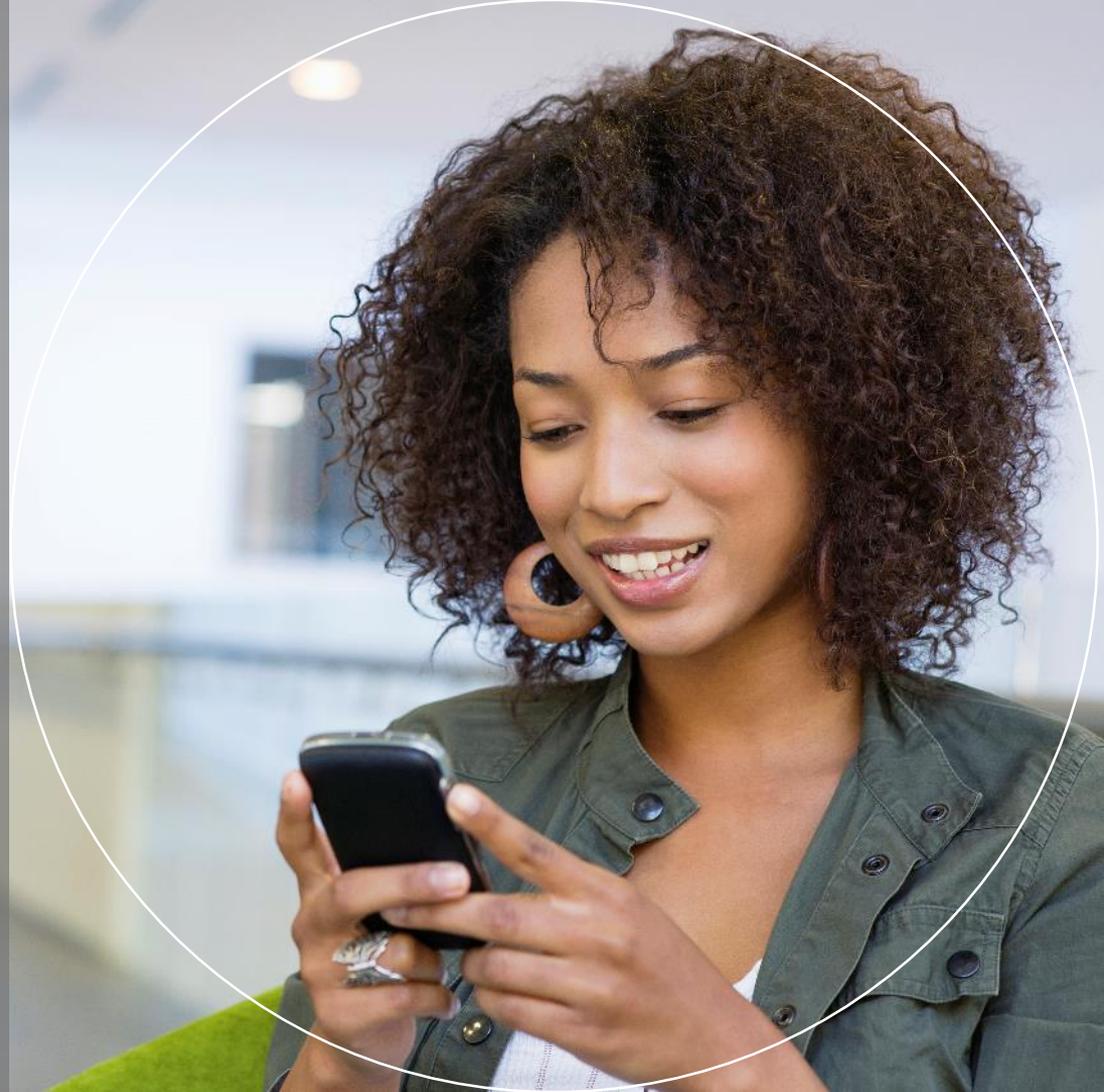
EMV 3-D Secure

Mastercard
Identity Check





3. Mastercard's Authentications strategy



What is Mastercard's authentication strategy in Europe?

The focus for Mastercard, its customers and all the players in the payment ecosystem should be on providing secure, simple and seamless Cardholder experiences that balance the new requirements against the friction of authentication.

Mastercard's objectives are:

1) To drive e-commerce conversion and approval rates up.

This can be achieved with a seamless authentication experience and biometrics.

2) To increase security.

This can be achieved with effective risk-scoring, which provides a layered approach to security and allows for one-click payments.

3) To help customers apply the exemptions.

This can be achieved with changes in our rules that facilitate the application of the exemptions.

What is Mastercard's authentication strategy in Europe?

Seamless SCA for higher conversion and approval rates

SCA is effective if used with a best in class consumer experience. A seamless authentication solution through any device, any Merchant and any Cardholder is key. This will drive e-commerce conversion and approval rates up and increase transaction volumes.

Mastercard® Identity Check™ provides such a seamless authentication experience across payment environments and devices (face-to-face and e-commerce, in-app and within websites, Internet of Things). Mastercard Identity Check implements the EMV® 3-D Secure (3DS) global industry standard for authentication.

With biometrics, Mastercard Identity Check allows Cardholders to securely pay with one single touch. This will drive e-commerce approval rates to the level of face-to-face or even higher. Mastercard has developed other biometrics solutions that provide a seamless consumer experience (e.g., Masterpass and DSRP).

What is Mastercard's authentication strategy in Europe?

Risk-scoring for security and one-click payments

Mastercard's authentication strategy consists of a layered approach. By layering security approaches, such as effective risk-scoring, alongside an actual authentication, much greater security can be obtained.

Risk-scoring takes advantage of information that is available at or before authentication and during authorization. The use of device information, geo or IP location, behavioural biometrics, and scoring using Artificial Intelligence provide a wealth of opportunities to determine the risk associated with a transaction.

The regulation mandates risk-scoring for each transaction. If the risk is low and an exemption applies, SCA is not required. This makes one-click payments still possible under the new regulation.

In order to achieve a complete risk-scoring, the best solution is for the Merchant to provide the Issuer with information about the transaction, including its own risk-scoring. In this way, the Issuer may assess the risk of a transaction and, if the risk is low and an exemption applies, decide not to apply SCA.

What is Mastercard's authentication strategy in Europe?

Mastercard's authentication infrastructure

Mastercard is driving the development of the infrastructure to support the new authentication requirements. Support for customers is in place and being communicated through bulletins.

Mastercard has changed its e-commerce consumer-facing authentication brand from Mastercard SecureCode to Mastercard® Identity Check™. The new brand better reflects our new authentication solution, with its emphasis on biometrics and ban on static authentication.

Mastercard is also developing innovative authentication solutions based on behavioural biometrics.



4. Exemptions



Optimising the use of exemptions

Even though a transaction falls within the scope of the PSD2 RTS a number of exemptions exist that mean certain transactions are not subject to the requirement for SCA. Identifying and optimising the use of these exemptions will help to deliver a frictionless consumer shopping experience.

Exemption	Sources
Transaction Risk Analysis (TRA)	Article 18 RTS
Commercial transactions	Article 17 RTS
White list of trusted beneficiaries	Article 13 RTS
Recurring transactions	Article 14 RTS
Low-value remote transactions	Article 16 RTS
Contactless payment	Article 11 RTS
Unattended terminals for transit and parking	Article 12 RTS

Some exemptions can only be applied by certain parties and provided PSD2 RTS conditions are met.

SCA exemptions – overview

In scope of the RTS for SCA

Out of scope

Acquirer PSPs

Issuer PSPs

Low-value transactions - LVP (art 16)
≤30 EUR - with counter limitation for Issuers

Transaction risk analysis – TRA (art 18)
*if fraud ≤ 13 bps up to 100€
if fraud ≤ 6bps up to 250€
if fraud ≤ 1bps up to 500€*

Recurring transactions (art 14)
- same amount, same payee

White listing of trusted beneficiaries (art 13)

Secure corporate payments (art 17)

Anonymous prepaid cards

Mail Order/Telephone Order - MOTO

'One-leg' transactions

Merchant-initiated transactions - MIT

Acquirer and Issuer Exemptions

Article 16 RTS: Low value payments (LVP) are defined by PSD2 RTS as 'low value' if less than or equal to €30 or equivalent in other currencies.

However, even low value payments require authentication for every sixth transaction, or if the cumulative amount is higher than €100 since the last SCA.

Acquirer and Issuer Exemptions

Article 18 RTS: Transaction Risk Analysis (TRA) due to low fraud rate. Available for transactions for which the amount and fraud level do not exceed pre-defined limits as per the RTS. The amount varies depending on the fraud levels (see diagram below) and is not subject to any counter limitations.

Transaction size	Provided that acquirer's fraud rate* is no more than
Up to €500	0.01%
Up to €250	0.06%
Up to €100	0.13%

The fraud rate is defined as the total value of unauthorised and fraudulent remote card transactions, divided by the total value of all remote card transactions.

In practical terms, an Acquirer should consider using an exemption under Transaction Risk Analysis (TRA) where the Merchant is sufficiently happy with a consumer's transaction history and other known variables that they are confident that the transaction is not fraudulent. However, it should be remembered that it is the Issuer that has the final decision and has the right to turn down the request and to request SCA.

Acquirer and Issuer Exemptions

Article 14: Recurring Transactions if the amount and the payee is the same.

However, SCA is required when creating the initial recurring payment agreement including a correct setting of the amount, expiration and frequency of the recurrence. It is also necessary when amending a recurring payment. Subsequent recurring transactions shall include reference to the initial agreement.

Issuer Exemptions

Article 13 RTS: White-listing of trusted beneficiaries – A Cardholder can request their Issuer to white-list a Merchant so that SCA is not required on subsequent transactions to that Merchant. Merchants that have been listed by Cardholders are known as ‘trusted beneficiaries’. SCA is however, always required for the creation or amendment of the white-list.

Issuers and Access Control Server (ACS) providers have an important role to play by making it simple for the Cardholder to white-list a Merchant while shopping.

For example, a Cardholder could be presented with the option to add a Merchant to a white-list

- per Merchant, during payment - white-listing prompt on authentication page
- per Merchant, after payment – white listing prompt on separate page
- multiple Merchants – white listing via mobile bank

Mastercard has produced Standards for Merchant White-Listing. *Ask your Acquirer or your Mastercard representative for more information.*

Issuer Exemptions

Article 17 RTS: Secure Corporate Payments or Business to Business (B2B) payments over dedicated payment processes or protocols are exempted if they are only available to payers who are not consumers where competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those achievable with SCA.

Although this decision lies with the competent authority of each member state, lodged and virtual corporate/commercial cards may be exempted. However, as this is not an Acquirer applied exemption Merchants should always send an authentication request and it is the responsibility of the Issuer to inform their Access Control Server (ACS) of card numbers or ranges that can use this secure corporate payment SCA exemption to avoid a step up. It should be noted that the use of a commercial card by an employee at a public website for the purchase of goods and services is not exempted as the transaction does not use a secure dedicated payment process and protocol.

Issuer Exemptions

Article 11 RTS: Contactless transactions in the Face to Face domain offer the best card payment experience but SCA requirements can affect it. Under Article 11 contactless transactions are exempt where:

- the individual transaction is no more than €50;
- and the cumulative amount of previous contactless transactions since the last SCA is less than €150,
- or the number of consecutive transactions since the last SCA does not exceed five.

Mastercard aims to improve the Cardholder experience for contactless transactions performed using a card or non-card form factor when the Issuer host needs to request SCA as a result of tracking Article 11 exemptions as defined in the PSD2 RTS on SCA.

Further details and clarification speak to your Acquirer or your Mastercard representative..

Issuer Exemptions

Article 12 RTS: Unattended terminals for transit and parking SCA is not required for contact or contactless transactions for paying a transport fare or parking fee at unattended payment terminals, regardless of amount. This is not a general exemption for all unattended terminals.

For avoidance of doubt...

SCA is always needed for the following transactions:

- ✓ Adding a card to a Merchant's file (Card on File)
- ✓ Starting a recurring payment arrangement for fixed and variable amounts, including Merchant Initiated Payments
- ✓ White-Listing (or viewing/amending White-Lists)
- ✓ Binding a device to a Cardholder





5. Your Communication Toolkit



Communicating with impact: Your Mastercard® Identity Check™ communication toolkit

This communication toolkit has been designed help you effectively provide your customers with information about Mastercard® Identity Check™ - with the objective to support a successful transition and uninterrupted services.

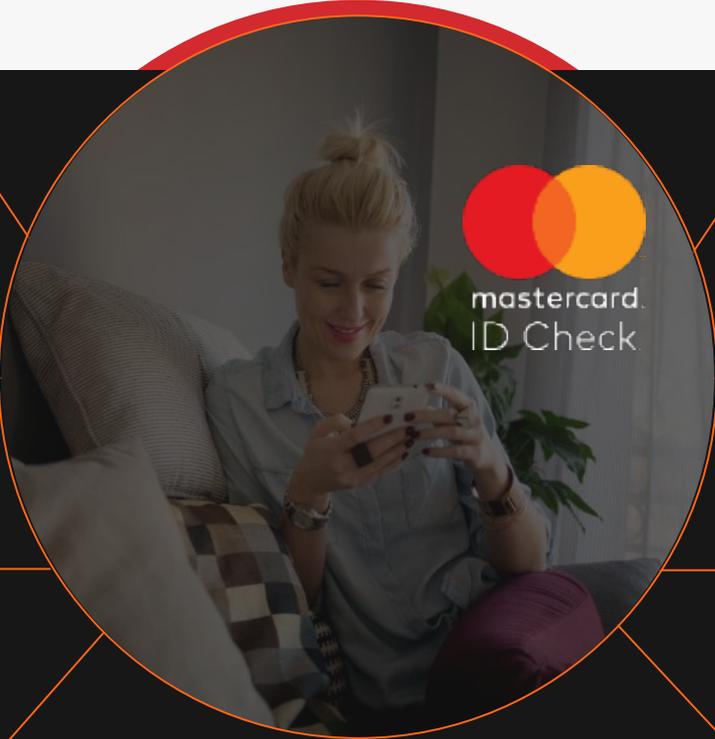
It provides assets for key consumer touchpoints used to communicate about Mastercard Identity Check and enable Cardholders to seamlessly use their Mastercard® card for electronic payments after September 14, 2019.

You can mix and match toolkit elements to customise messages for specific audience and channel requirements. You can either populate the templates provided, or use them as a basis to develop your own content or designs.

In any case you should modify the content according to your individual value proposition and needs of your Cardholders. Remember to always add your logo, contact details and any other information you may need to include before your communication undergoes a final legal check with your advisor.

Supporting you to educate your customers through your own communication channels

Mastercard Identity Check toolkit overview



1 Key Messages

2 Key Visuals

3 Design Templates

4 Website Content

5 FAQs / Help pages

6 User Journeys

7 Information Video

8 Mastercard Brand

What your customers need to know

Making changes to the payment verification process can effect consumer sentiment and conversion. Clear explanation of what is changing and how they can avoid interruption will help to mitigate business risk.

Consumers will want to know:

- ✓ Why the changes are coming
- ✓ What will be different
- ✓ When the changes will be introduced
- ✓ How their online purchase journey will be affected
- ✓ What they can do to be ready



Connect with your consumers and guide them through all phases of the transition - with your customised communication plan



1 Key Messages that empathise and engage

Key messages for Mastercard® Identity Check™ work by setting out value promises that draw readers in, make them want to know more, and provide them with all necessary information about the new user experience, its benefits and possible actions to take with their Issuer.

Over the following pages, you'll find a wide selection of headlines and copy to use as you see fit, together with an outline of all the assets available to you. Select the ones that best reflect your position and adapt them according your individual needs, communication channels and target group.

Headlines that empathise and engage

CHOICE OF HEADLINES

A. Enhanced Security

B. Easy Checkout

C. Peace of Mind

D. Across Every Device

Customizable copy that's informative and concise

COPY TEMPLATES 'MEDIUM'

A. Convenient & Secure Online Payments

B. Easy Checkout

C. New Era of Safety in Digital Payments / Regulation

Customizable copy that's detailed and aspirational

COPY TEMPLATES 'LONG'

Convenient & Secure Online Payments, Easy Checkout, Regulation / New Standards, Advanced Authentication Technology, How it works

Value Pillar

A. Enhanced security: Mastercard® Identity Check™ uses advanced technology to make online payments with Mastercard® cards more secure. We as a Merchant cooperate with card Issuers to help them evaluate every online payment in real time and either approve it instantly or – if an extra layer of security is needed – ask for confirmation of the Cardholder’s identity to protect the purchase.

Emotional Benefit

Protection

Headlines

- **Protect your online purchases with Mastercard® Identity Check™**
- **Enjoy a simple and secure online shopping experience!**
We use the advanced technology of Mastercard® Identity Check™
- **Digital payment security unique to you**
Use state-of-the-art technology for a smart checkout experience
- **Mastercard® Identity Check™:** Get state-of-the art protection for your online payments
- **Get extra protection when you pay online**
Protect your purchase with enhanced security provided by Mastercard® Identity Check™

Value Pillar

B. Easy checkout / fewer passwords: Checking out is now as simple and secure as never before. We're using advanced technology to make your online payments with Mastercard® safer, faster and more convenient – in close cooperation with your card-issuing bank. How? Static passwords – that are hard to remember or easy to guess – are replaced by biometric authentication methods, SMS one-time passcodes or other familiar methods of verification from your bank, so you always know what to do and can enjoy a seamless checkout.

Emotional Benefit

Simple user experience

Headlines

- **Simplify your checkout experience with Mastercard® Identity Check™**
- **Mastercard® Identity Check™**: Use smart authentication to protect your online purchases
- **Mastercard® Identity Check™**: Use smart technology for a safe and simple digital payment experience
- **Mastercard® Identity Check™**: Get advanced online payment protection that's easy to use
- **Mastercard® Identity Check™**: Enjoy simpler online payments with added peace of mind

Value Pillar

C. Peace of mind / Get prepared [CTA]: Mastercard® Identity Check™ is an advanced authentication solution to make your online payments simpler and safer, any time, across all your devices. It helps protect your online Mastercard® payments from fraud without complicating your digital payment experience. It's sophisticated, yet simple, for greater peace of mind.

Emotional Benefit**Trust****Headlines**

- **Enjoy peace of mind when paying online with Mastercard® Identity Check™**
- **Your peace of mind when paying online**
Talk to your card-issuing bank now to get state-of-the-art payment protection working for you
- **Use advanced technology to enjoy peace of mind when paying online**
Talk to your bank now to stay protected every time
- **Sophisticated yet simple online shopping? With Mastercard® Identity Check™**
You get the peace of mind you deserve. Talk to your bank now to check if you're ready to go
- **Mastercard® Identity Check™: Smart security for smart payments.**
Talk to your bank now to stay protected every time

Value Pillar

D. Across every device: Shopping on your mobile, paying bills on your laptop or booking tickets on your tablet? No matter which device you use, Mastercard® Identity Check™ makes your online payments simpler and safer, any time, anywhere.

Emotional Benefit

Flexibility / Mobile optimisation

Headlines

- **Pay securely on any device with Mastercard® Identity Check™**
- **Mastercard® Identity Check™: Enjoy strong security standards when shopping online – any time, anywhere on any connected device**
- **Mastercard® Identity Check™: Simple and secure online payments on every device**
- **Mastercard® Identity Check™: Enjoy the same safe and secure online payment experience on every device you use**
- **Stay safe when paying online – Mastercard® Identity Check™ offers personalised security on every device**

A. Convenient and Secure Payments

Enjoy a more convenient and secure online shopping experience – with Mastercard® Identity Check™

Today, we need payments in the digital world to be as safe and smooth as they are in-store. Security needs to move with the times – and so does convenience. That's why we've implemented Mastercard Identity Check – an advanced solution to make your online payments simpler and safer, any time, across all your devices. As of September, when you use your Mastercard® card, you'll benefit from:

- **Enhanced security:** Protect your purchases with an additional layer of security
- **Flexibility:** Enjoy the same safe and secure experience across every device you use
- **Easy checkout:** Simplify your checkout experience by eliminating complicated passwords

How does it work? Mastercard Identity Check leverages state-of-the-art technology to help your card-issuing bank check your identity when you make online payments with your Mastercard card at our shop. This means all payments are checked in real time, with most approved by your bank instantly and 'invisibly', making your experience smooth and convenient. When an extra layer of security is needed, at our checkout you will be asked to confirm your identity – for example by entering a one-time passcode that you receive by SMS, by confirming the purchase with your fingerprint in your banking app or by using another familiar method of verification from your bank. It's that simple.

Next steps: Contact your card-issuing bank to make sure you're fully set for the more secure way to pay and that you can continue using your Mastercard card for online payments without any interruption. Some banks require a registration from your side or ask you to update information e.g. your mobile number and/or email address.

Enjoy peace of mind knowing that your purchase is protected with enhanced security provided by Mastercard Identity Check.

More information?

- Please visit our help page or contact customer service at customerservice@sampleMerchant.com or 000 – 000000 [pls. enter links/information/contact details].
- Please speak to your bank to find out more about the authentication methods they offer and if you're all set to continue using your Mastercard card or online payments after September 2019

B. Smart Authentication Technology

Smart authentication that protects your online purchases – with Mastercard® Identity Check™

As our customer and Mastercard Cardholder, you can now benefit from enhanced protection that makes your online payments simpler and safer, any time, across all your connected devices. We've implemented Mastercard Identity Check – an advanced solution that brings you the latest authentication technology to protect your online payments from fraud, without complicating your digital payment experience.

Mastercard Identity Check helps us to better cooperate with your card-issuing bank to make your online checkout experience faster, more secure and more convenient. We help them verify that your purchases are truly yours – with as little input and disruption for you as possible. Whenever an extra layer of security is required, you simply authenticate your purchase quickly and conveniently with your bank – for example by entering a one-time passcode that you receive by SMS, by confirming the purchase with your fingerprint in your banking app or by using another familiar method of verification from your bank. Speak to your bank to find out more about the authentication method they offer.

Here's how it works:

- When you click on 'Confirm Order' at our checkout page, the transaction is automatically assessed in real time
- Some transactions can be approved by your bank directly. Only if an additional layer of security is needed, you'll be prompted to authorise the payment
- If your bank uses biometric authentication: you open the app via the push notification on your mobile phone (no matter what device you used to place the order online) and approve the payment by using your fingerprint
- If your bank uses one-time passcodes: in the Mastercard Identity Check pop-up, enter the one-time passcode (OTP) which you will receive by SMS on your mobile phone (or at the email address you registered with your bank)
- We will receive this confirmation and your order will be complete
- That's it! No passwords to remember, and it's still simple and secure

Mastercard Identity Check enhances your online checkout experience by eliminating complicated passwords and focusing on who you are, not what you know. Learn more [[enter link to more information / FAQs](#)].

Make sure you can enjoy the new safe and secure experience without any disturbance in your shopping experience. Please check with your bank if you're all set for the change and able to use Mastercard Identity Check seamlessly after September 2019.

C. New Era of Safety in Digital Payments

Mastercard® Identity Check™ : State-of-the art protection for your online payments

We're entering a new era of safety and convenience when shopping online with your Mastercard® card. Helping you make the most of these changes is Mastercard Identity Check, a new approach that puts you at the centre of the authentication process.

There are three key ways Mastercard Identity Check will improve digital payments with your Mastercard card:

- 1. Smooth and secure checkout experience.** An updated global industry standard (EMV® 3-D Secure) and new European legislation enables us to cooperate closer with banks and let them better evaluate each payment in real time. With the result that they can approve standard payments 'invisibly', only requiring you to confirm your identity when an additional layer of security is needed.
- 2. Who you are, not what you remember.** Advanced authentication tools mean you no longer need to remember complicated passwords – instead you can simply use a tap of your finger, a smile, a one-time passcode that your bank sends to your mobile phone or another familiar method of verification from your bank to confirm your payment.

To enhance security and follow new legislation your bank will check a combination of two out of three different factors that are independent:

- Something you know (e.g. a password)
- Something you have (e.g. your mobile device) or
- Something you are (e.g. your fingerprint)

This method of confirming your identity is called 'two-factor authentication' or 'Strong Customer Authentication (SCA)'. Mastercard Identity Check facilitates this advanced approach to payment security and puts you at the centre of the authentication process, no matter what device you use.

- 3. Mobile optimisation.** Mastercard Identity Check is an advanced solution to make your online payments safe and smooth, any time, across all your devices – with a consistent experience no matter which device you use to shop, book and pay online.

Mastercard Identity Check replaces SecureCode™ providing you with state-of-the-art protection when you pay online while making your checkout experience easier, faster and safer. It is designed to work with today's cutting-edge technologies, but is future-ready to protect your purchases today and tomorrow.

Benefit from an advanced solution and speak to your bank to make sure your card is ready to be used with Mastercard Identity Check. Old SecureCode will no longer be needed during checkout. [Find out more](#) about how to benefit from advanced protection when paying online [*enter link to more information / FAQs*]

Get state-of-the-art technology for a seamless and secure online check out experience – with Mastercard® Identity Check™

Your digital payments with Mastercard® are about to become more secure and more convenient. New European legislation for online payments and authentication, combined with state-of-the-art technologies will change the way you pay online, providing enhanced security that's simple to use.

As of September [enter date], when you use your Mastercard® card online, your bank might ask you to verify your identity to make sure that it's really you making the purchase. It's a simple step that enhances your online payment security, no matter which device you happen to be using.

Smart authentication protects your online purchases

The new European legislation makes it a requirement to use extra levels of authentication to make online payments more secure and help protect you from fraud. This means that additional information, like a one-time passcode or your fingerprint might be required at checkout, after you've entered your card number, expiry date and CVC verification code. There are exceptions, but you need to be prepared to ensure you can complete your transaction.

Mastercard Identity Check helps your bank verify that it's really you making the purchase. It's an advanced authentication solution that leverages state-of-the-art technology to make online payments with your Mastercard card safe and smooth – any time, across all your devices.

- 1. Smooth check out:** All e-commerce payments are checked in real time, and most are approved directly by your bank without anything more needed from you.
- 2. Enhanced security:** If an additional layer of security is needed, your bank will instantly ask for verification to make sure the purchase is really yours.
- 3. Anywhere – any time – any device:** Enjoy the same experience, on every connected device you use.

1. Smooth check out: It's sophisticated, yet simple – for greater peace of mind

The advanced technology behind Mastercard Identity Check is based on an improved global industry standard (EMV® 3-D Secure) and enables your bank to evaluate every transaction in real time, using relevant data points to verify that your purchases are truly yours. If they can be confident that it's really you initiating the payment with your Mastercard card, it'll be approved directly to make your check out experience as fast and seamless as possible. However, if an additional layer of security is needed to protect your purchase, at checkout you'll be asked to prove it's really you making the payment.

(...)

(...)

2. Enhanced Security: Protect your purchases with an additional layer of security

In the event that a payment needs to be verified, the new legislation will require your bank to check a combination of two out of three different factors that are independent:

- Something you know (e.g. a password)
- Something you have (e.g. your mobile device) or
- Something you are (e.g. your fingerprint)

For example, you can combine 'something you own' such as your mobile phone, with 'something you are' like your fingerprint. There are numerous possibilities and combinations – and more choice means better authentication experiences, with less friction.

This method of confirming your identity is called 'two-factor authentication' or 'Strong Customer Authentication (SCA)'. Mastercard Identity Check facilitates this advanced approach to payment security and puts you at the centre of the authentication process, no matter what device you use.

3. Anywhere – any time – any device: Stay safe when paying online and enjoy personalised security on every device

Shopping on your mobile, paying bills on your laptop, or booking tickets on your tablet, with Mastercard Identity Check you can enjoy the same safe and secure experience, no matter which device you use.

The new, advanced authentication process with Mastercard Identity Check is optimised for mobile devices. It eliminates the need to remember multiple passwords and complex information. No one wants to type complex passwords including numbers and special characters into mobile devices to complete a purchase, and who can remember all this information? Instead you can just use, for example, a tap of your finger, your smile or a one-time passcode that your bank sends to your mobile phone to confirm your payment and you're good to go. It's easier, faster and more secure.

You'll find the Mastercard Identity Check logo on our website – it's the sophisticated yet simple way to protect your payments.

(...)

Enjoy peace of mind knowing that your online purchases are protected with advanced security provided by Mastercard Identity Check

Mastercard Identity Check provides extra protection when paying online. It helps your bank to verify that your purchases are truly yours by authenticating your identity quickly and conveniently. Furthermore, Identity Check is designed to work with today's cutting-edge technologies, but is future-ready to make your online shopping experience faster and more secure today and tomorrow.

Benefit from added protection that helps simplify and secure online payments. Learn more [enter link to more information] about the new requirements and how Mastercard Identity Check enables you to complete your online payments in line with the new regulation.

Switch to smart authentication to protect your online purchases – with Mastercard Identity Check

We recommend you check with your bank if you need to **register your card** with their Mastercard Identity Check programme, so that you can complete your online payments with the required authentication after the new standard applies.

You might also want to check if your bank has your correct details in their records e.g. your phone number to send you a one-time passcode or that you've downloaded their banking app that may be needed for biometric authentication. Ask your bank about the authentication method they're offering and what is needed to get upgraded to the new standard in online payments.

Mastercard Identity Check replaces SecureCode™ providing you with state-of-the-art protection when you pay online while making your checkout experience easier, faster and safer. SecureCode will no longer be needed during our checkout.

Get advanced online payment protection that's easy to use. For more information please [click here](#) [insert link] or contact us on xxxxxxxxxx [enter number].

2 Key visuals: "Mastercard® Identity Check™"

Mastercard has developed a number of images illustrating the Cardholder authentication experience with Mastercard Identity Check when making card-not-present (CNP) e-commerce purchases. They are based on Mastercard's EMV® 3DS 2.1.0 / SCA User Experience Recommendations and can be used across all communication materials.

They are available for the four major use cases that Cardholders will face:

FRictionLESS CHECKOUT

In this instance, the Cardholder is not challenged with an authentication request e.g. as a result of the Issuer assessment on the low risk of the transaction

OUT OF BAND *Single device*

The Out of Band (OOB) checkout flow allows for Issuer authentication to occur outside of the Merchant shopping environment. This section describes where the same device is used for both the purchasing transaction and authentication

OUT OF BAND *Multiple devices*

As an extension of OOB single device, here two different devices are used: one for shopping (a desktop browser in this case) and one for authenticating the transaction via a separate authentication application (app). This flow sets out Mastercard's requirements to cover this scenario

OTP via SMS*

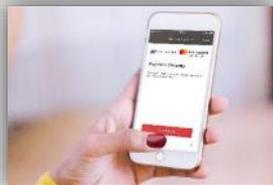
If the Cardholder does not have (i) an authentication app installed, (ii) does not have a device capable of supporting such an app or (iii) the Issuer is not offering biometric authentication, here we show how the transaction can be authenticated using a OTP sent via SMS to the Cardholder's registered mobile number

2 Key visuals: "Mastercard® Identity Check™"

FRictionless CHECKOUT



OUT OF BAND *Single device*



OUT OF BAND *Multiple devices 'tablet'*



OUT OF BAND *Multiple devices 'laptop'*



One-Time- Passcode (OTP) via SMS



2 Key visuals: "Mastercard® Identity Check™"

FRICTIONLESS CHECKOUT

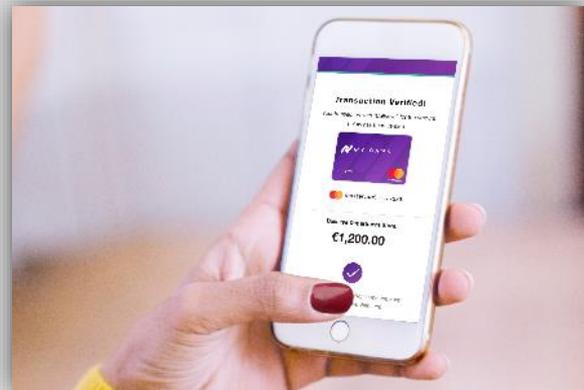
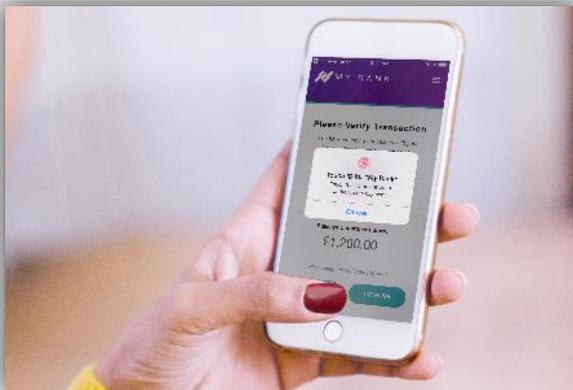
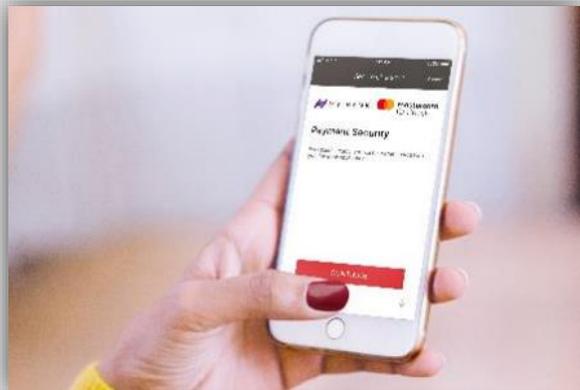
In this instance, the Cardholder is not challenged with an authentication request e.g. as a result of the Issuer assessment on the low risk of the transaction



2 Key visuals: "Mastercard® Identity Check™"

OUT OF BAND
Single device

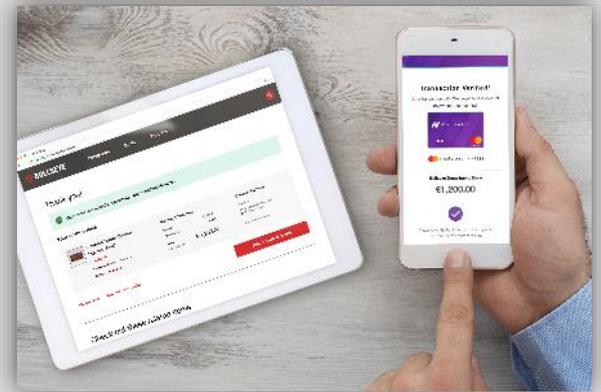
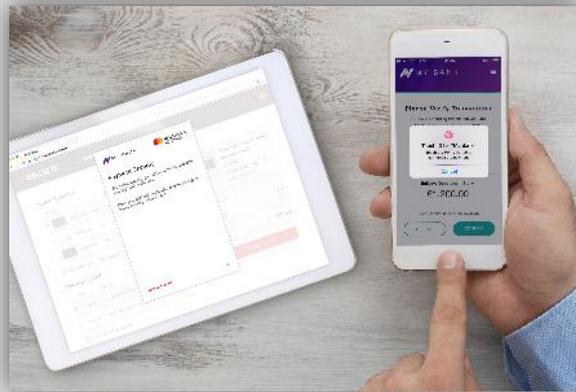
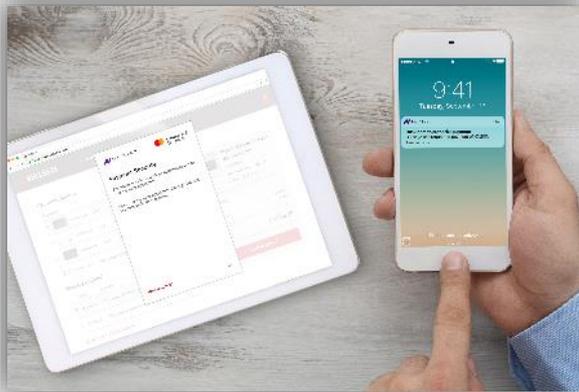
The Out of Band (OOB) checkout flow allows for Issuer authentication to occur outside of the Merchant shopping environment. This section describes where the same device is used for both the purchasing transaction and authentication



2 Key visuals: "Mastercard® Identity Check™"

OUT OF BAND
Multiple devices

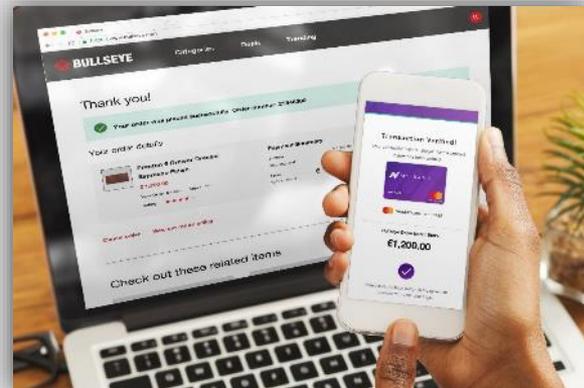
As an extension of OOB single device, here two different devices are used: one for shopping (a desktop browser in this case) and one for authenticating the transaction via a separate authentication application (app). This flow sets out Mastercard's requirements to cover this scenario



2 Key visuals: "Mastercard® Identity Check™"

OUT OF BAND
Multiple devices

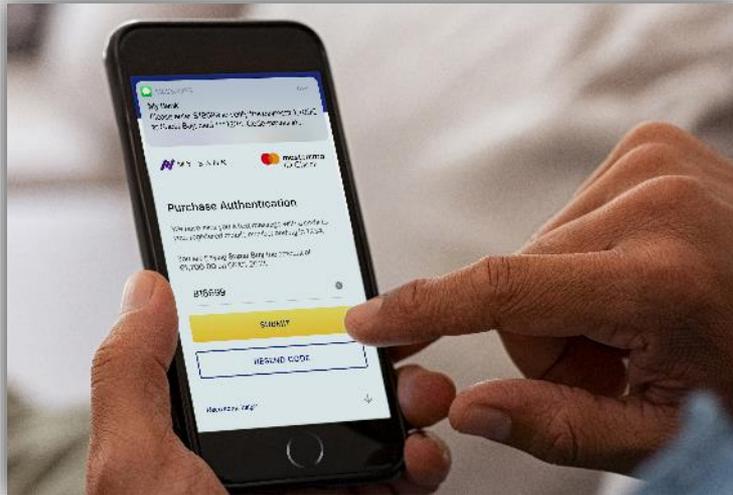
As an extension of OOB single device, here two different devices are used: one for shopping (a desktop browser in this case) and one for authenticating the transaction via a separate authentication application (app). This flow sets out Mastercard's requirements to cover this scenario



2 Key visuals: "Mastercard® Identity Check™"

OTP via SMS

If the Cardholder does not have (i) an authentication app installed, (ii) does not have a device capable of supporting such an app or (iii) the Issuer is not offering biometric authentication, here we show how the transaction can be authenticated using a OTP sent via SMS to the Cardholder's registered mobile number



* OTP SMS MAY REQUIRE AN ADDITIONAL KNOWLEDGE FACTOR (LIKE PASSWORD, PIN OR SECURITY QUESTION) TO COMPLY WITH THE EBA REGULATORY TECHNICAL STANDARDS (RTS)

Email / Newsletter

Marketing Insert / Flyer

Digital Advertising

Social Media



Introducing extra protection when you pay online – with Mastercard® Identity Check™

Dear [customer],

Today, we need payments in the digital world to be as safe and smooth as they are in-store. Security needs to move with the times – and so does convenience.

That's why we've implemented **Mastercard Identity Check** – an advanced solution to make your online payments simpler and safer, any time, across all your devices.

As of today, when you use your Mastercard® card online you'll benefit from:

- Enhanced security:** Protect your purchases with an additional layer of security.
- Flexibility:** Enjoy the same safe and secure experience across every device you use.
- Easy checkout:** Simplify your checkout experience by eliminating complicated passwords.

This service is offered free of charge and doesn't require any registration from your side, you are automatically enrolled.

How does Mastercard Identity Check work?

Mastercard Identity Check leverages state-of-the-art technology to help us verify that your purchases are truly yours, to protect you from fraud and false declines. This means all payments are checked in real time, with most approved instantly and "frictionlessly", making your experience smooth and convenient. When an extra layer of security is needed, at checkout, you will be asked to confirm your identity with your fingerprint in our banking app. It's that simple.

Get advanced online payment protection that's easy to use. For more information please click [here](#) (insert link) or contact us on [\(insert phone\)](#).

[signature]

Learn more

Introducing a more convenient and secure online shopping experience – with Mastercard® Identity Check™

Today, we need payments in the digital world to be safe and smooth as they are in-store. That's why we've implemented Mastercard Identity Check – an advanced solution to make your online payments simpler and safer any time, across all your devices.

As of 11 September when you use your Mastercard® card online you'll be protected with an additional layer of security while enjoying a more convenient checkout experience.

Contact your local issuing bank to make sure you're fully set for the more secure way to pay and that you can continue using your Mastercard® card for online payments without any interruptions.

mastercard | Partner logo

Mastercard Identity Check™ is an advanced authentication solution that leverages state-of-the-art technology to help verify that your purchases are truly yours.

Smooth checkout: All e-commerce payments are checked in real time and most are approved directly on the checkout flow, reducing time needed from you.

Enhanced security: An additional layer of security for mobile, your card issuing bank will use biometric push for an app to help make sure the purchase is really yours.

Anywhere – any time – any device: Enjoy the same secure and convenient service on every connected device you use.

mastercard | Partner logo



Enjoy peace of mind knowing that your purchase is protected with advanced security provided by Mastercard Identity Check.

Learn more by visiting www.mastercard.com/help or contact your card-issuing bank.

©2018 Mastercard. All rights reserved. TM, ® 2018 Mastercard.

Introducing extra protection when you pay online: Mastercard® Identity Check™

mastercard | Partner logo

Sign up now

Smart authentication that protects your online payments Mastercard® Identity Check™

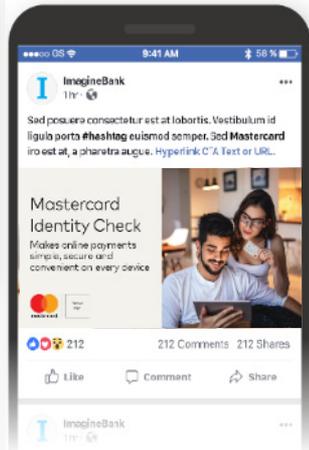
Sign up now

mastercard | Partner logo

Simple and secure online payments on every device: **Mastercard® Identity Check™**

Sign up now

mastercard | Partner logo



facebook

twitter



Instagram

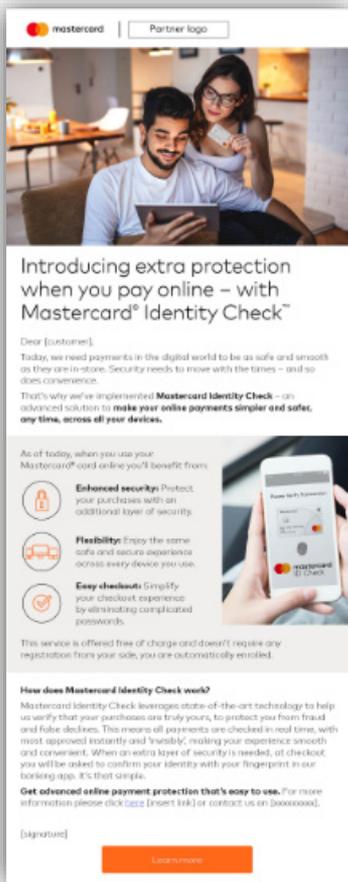
Mastercard Identity Check

Makes online payments simple, secure and convenient on every device

mastercard | Partner logo

The toolkit contains editable files to allow customisation.

Please contact your Acquirer or Mastercard representative for source files and to discuss availability of translated copy.



Sample copy ,Customer Information'

Introducing extra protection when you pay online – with Mastercard® Identity Check™

Dear [Customer],

Today, we need payments in the digital world to be as safe and smooth as they are in-store. Security needs to move with the times – and so does convenience.

That's why we've implemented **Mastercard Identity Check** – an advanced solution to make your online payments **simpler and safer, any time, across all your devices.**

As of today, when you use your Mastercard® card online you'll benefit from:

- **Enhanced security:** Protect your purchases with an additional layer of security
- **Flexibility:** Enjoy the same safe and secure experience across every device you use
- **Easy checkout:** Simplify your checkout experience by eliminating complicated passwords

This service is offered free of charge and doesn't require any registration from your side, you are automatically enrolled.

How does Mastercard Identity Check work?

Mastercard Identity Check leverages state-of-the-art technology to help us verify that your purchases are truly yours, to protect you from fraud and false declines. This means all payments are checked in real time, with most approved instantly and 'invisibly', making your experience smooth and convenient. When an extra layer of security is needed, at checkout you will be asked to confirm your identity with your fingerprint in our banking app. It's that simple.

Get advanced online payment protection that's easy to use. For more information please click here or contact us on xxxxxxxxx.

[Signature]

[Learn more](#)

3 Design Templates: Marketing Insert / Flyer

Introducing a more convenient and secure online shopping experience – with Mastercard® Identity Check™

Today, we need payments in the digital world to be safe and seamless at the same time. That's why we've implemented Mastercard Identity Check – an advanced solution to **make your online payments simpler and safer, any time, across all your devices.**

As of 1st September when you use your Mastercard® card online you'll be protected with an additional layer of security while enjoying a more convenient checkout experience.

Contact your card-issuing bank to make sure you're fully set for the more secure way to pay and that you can continue using your Mastercard card for online payments without any interruption.



Mastercard® Identity Check™ is an advanced authentication solution that leverages state-of-the-art technology to help verify that your purchases are truly yours.

Smooth checkout: All e-commerce payments are checked in real time, and most are approved directly without anything more needed from you.

Enhanced security: If an additional layer of security is needed, your card-issuing bank will instantly ask you for verification to make sure the purchase is really yours.

Anywhere – any time – any device: Enjoy the same experience on every connected device you use.



©2018 Inge & Co. 1231 Westlawn Cir. #1200, N.Y. 10019

Enjoy peace of mind knowing that your purchase is protected with enhanced security provided by Mastercard Identity Check.

Learn more by visiting www.sampleretailer.com/help or contact your card-issuing bank.

Sample copy 'Customer information in advance'

Introducing a more convenient and secure online shopping experience – with Mastercard® Identity Check™

Today, we need payments in the digital world to be safe and seamless at the same time. That's why we've implemented **Mastercard Identity Check – an advanced solution to make your online payments simpler and safer, any time, across all your devices.**

As of 14th September when you use your Mastercard® card online you'll be protected with an additional layer of security while enjoying a more convenient checkout experience.

Contact your card-issuing bank to make sure you're fully set for the more secure way to pay and that you can continue using your Mastercard card for online payments without any interruption.

Mastercard® Identity Check is an advanced authentication solution that leverages state-of-the-art technology to help verify that your purchases are truly yours.

- **Smooth checkout:** All e-commerce payments are checked in real time, and most are approved directly without anything more needed from you.
- **Enhanced security:** If an additional layer of security is needed, your card-issuing bank will instantly ask you for verification to make sure the purchase is really yours.
- **Anywhere – any time – any device:** Enjoy the same experience on every connected device you use.

Enjoy peace of mind knowing that your purchase is protected with enhanced security provided by Mastercard Identity Check.

Learn more by visiting www.sampleretailer.com/help or contact your card-issuing bank.

3 Design Templates: Internet Banner



Smart authentication that protects your online payments
Mastercard® Identity Check™

Sign up now



300x600



Get advanced protection for your online payments
Mastercard® Identity Check™

Sign up now



728x90

Simple and secure online payments on every device:
Mastercard® Identity Check™

Sign up now

300x250

Smart security for smart payments:
Mastercard® Identity Check™

Sign up now

Introducing extra protection when you pay online:
Mastercard® Identity Check™

Sign up now

Get state-of-the-art protection for your online payments:
Mastercard® Identity Check™

Sign up now

3 Design Templates: Internet Banner



Smart authentication that protects your online payments
Mastercard® Identity Check™

[Learn more](#)



300x600



Get advanced protection for your online payments
Mastercard® Identity Check™

[Learn more](#)



728x90

Simple and secure online payments on every device:
Mastercard® Identity Check™

[Learn more](#)



300x250

Smart security for smart payments:
Mastercard® Identity Check™

[Learn more](#)



Introducing extra protection when you pay online:
Mastercard® Identity Check™

[Learn more](#)



Get state-of-the-art protection for your online payments:
Mastercard® Identity Check™

[Learn more](#)



Hashtags

Approach 1:

Placing 'Mastercard® Identity Check™' in full uses a high number of characters for a hashtag, but the full version (3) is the easiest to read and understand compared to the abbreviated versions (1 and 2).

#MCIdentityCheck

#MastercardIDCheck

#MastercardIdentityCheck

Approach 2:

Break up the text with the brand's @ and separate Identity Check hashtag.

e.g. **@Mastercard® #IdentityCheck™**

They must always appear together as above, to ensure the full solution name "Mastercard Identity Check" is present.

3 Design / Copy Templates: Social Media / Facebook

facebook.

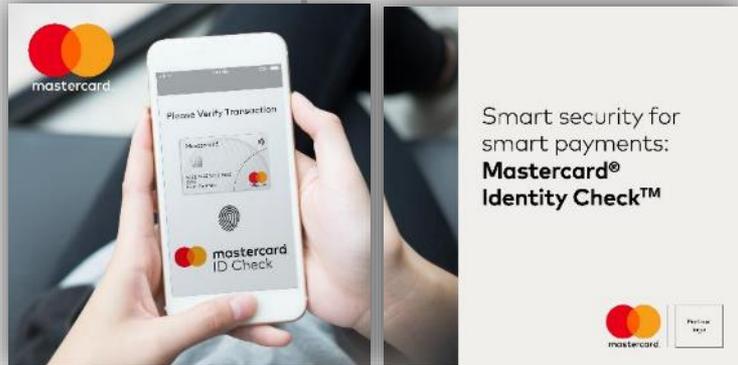
Smart authentication
that protects your
online payments
Mastercard®
Identity Check™



- Meet @Mastercard® #IdentityCheck™ and welcome a new era of authentication technology 🌱 Find out more today: [bit.ly link]
- Have you tried @Mastercard® #IdentityCheck™ yet? Upgrade today to the new standard for safe and smooth payments on every device 📱 Find out more: [bit.ly link]
- Meet @Mastercard® #IdentityCheck™ and welcome a new era of safety and convenience of online transactions 🌱 Find out more today: [bit.ly link]
- Have you tried @Mastercard® #IdentityCheck™ yet? Enjoy the same safe and smooth payment experience, whether you're shopping on your phone, laptop or tablet 📱 Find out more: [bit.ly link]
- Welcome to state-of-the-art authentication technology with @Mastercard® #IdentityCheck™ 🌱 Find out more today: [bit.ly link]



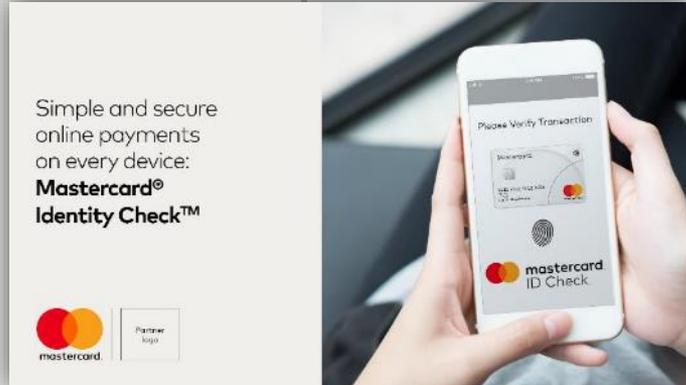
[with no image copy]



[with image copy – see Twitter copy]

- Shop online with peace of mind. Introducing @Mastercard® #IdentityCheck™ – the new standard for safe and smooth payments on every device 🛒
- Enjoy a smooth checkout experience. Upgrade to @Mastercard® #IdentityCheck™ – the new standard to keep your online payments safe 👍
- Get safe and smooth payments on every device. Introducing @Mastercard® #IdentityCheck™ – enjoy the same payment experience, whether you're shopping on your phone, laptop or tablet 🛒
- Shop online with peace of mind: welcome to a new era of authentication technology with @Mastercard® #IdentityCheck™ 🛒
- Enjoy a safe and smooth checkout experience: Upgrade to a new security standard for smooth online transactions with @Mastercard® #IdentityCheck™ 👍
- Get safe and smooth payments on every device: welcome to state-of-the-art payment technology with @Mastercard® #IdentityCheck™ 🛒

3 Design / Copy Templates: Social Media / Twitter



- Introducing @Mastercard #IdentityCheck – the new standard to confirm your payments when shopping online ✓ Find out more: [bit.ly link]
- Welcome to a new era of safety in digital payments! Welcome to @Mastercard #IdentityCheck. Find out more today: [bit.ly link]
- Introducing @Mastercard #IdentityCheck – the easy way to keep your online payments safe 🔒 Find out more [bit.ly link]
- Welcome to a new era of safety for online payments 🍉 Welcome to @Mastercard #IdentityCheck. Find out more today: [bit.ly link]
- Introducing @Mastercard #IdentityCheck – enjoy the same safe and smooth payment experience on all your devices 👍 Find out more: [bit.ly link]
- Welcome to state-of-the-art authentication technology 🍉 Welcome to @Mastercard #IdentityCheck. Find out more today: [bit.ly link]

4 Design / Copy Template: Your Landing Page



Enjoy a simple and secure online shopping experience: we use the advanced technology of Mastercard® Identity Check™

As our customer, you can now benefit from enhanced protection that makes your online payments simpler and safer, any time, across all your connected devices.

Introducing Mastercard Identity Check

An advanced solution that brings you state-of-the-art authentication technology to protect your online payments from fraud, without complicating your checkout experience.

With Mastercard Identity Check we help your bank verify that your purchases are truly yours

With as little input and disruption for you as possible, often making your online checkout experience even faster and more convenient. Whenever an extra layer of security is required, you simply authenticate your purchase conveniently with your bank in real time. For example by using a one-time passcode, your fingerprint or by another familiar method of verification from your bank. It's that simple.

The new European legislation makes it a requirement

To use extra levels of authentication to make online payments more secure and help prevent fraud. This will mean that as of 14th September 2019, just entering your card number and CVC verification code to confirm payments will no longer be sufficient. Make sure you're fully prepared and double check your mobile banking app and security settings.

Mobile optimisation

Mastercard Identity Check is an advanced solution to make your online payments safe and smooth, any time and across all your devices. It offers the same consistent experience no matter which device you use to shop, book and pay online.

If you have any questions, check out our [FAQ section](#) or [contact us](#).



Sample copy 'Customer Information'

Enjoy a simple and secure online shopping experience: We use the advanced technology of Mastercard® Identity Check™

As our customer, you can now benefit from enhanced protection that makes your online payments simpler and safer, any time, across all your connected devices.

Introducing Mastercard Identity Check – an advanced solution that brings you state-of-the-art authentication technology to protect your online payments from fraud, without complicating your checkout experience.

With Mastercard Identity Check we help your bank verify that your purchases are truly yours – with as little input and disruption for you as possible, often making your online checkout experience even faster and more convenient. Whenever an extra layer of security is required, you simply authenticate your purchase conveniently with your bank in real time. For example by using a one-time passcode, your fingerprint or by another familiar method of verification from your bank. [It's that simple.](#)

The new European legislation makes it a requirement to use extra levels of authentication to make online payments more secure and help prevent fraud. This will mean that as of 14th September 2019, just entering your card number and CVC verification code to confirm payments will no longer be sufficient. Make sure you're fully prepared and double check your mobile banking app and security settings.

Mobile optimisation Mastercard Identity Check is an advanced solution to make your online payments safe and smooth, any time and across all your devices. It offers the same consistent experience no matter which device you use to shop, book and pay online.

If you have any questions, check out our [FAQ](#) section or [contact us](#).

* NOT ALL AUTHENTICATION METHODS ALLOW TO ELIMINATE STATIC PASSWORDS. FOR EXAMPLE, OTP SMS MAY REQUIRE AN ADDITIONAL KNOWLEDGE FACTOR (LIKE PASSWORD, PIN OR SECURITY QUESTION) TO COMPLY WITH THE EBA REGULATORY TECHNICAL STANDARDS (RTS)

4 Design / Copy Template: Your Landing Page



How does it work?

With Mastercard® Identity Check™ we leverage state-of-the-art technology to help your card-issuing bank check your identity when you make online payments with your Mastercard® card at our shop.

This means all payments are checked in real time, with most approved by your bank instantly and 'invisibly', making your experience smooth and convenient.

No extra authentication needed



When an extra layer of security is needed, at our checkout you will be asked to confirm the payment – for example by entering a one-time passcode (sent via SMS) or using your fingerprint and your banking app or another familiar method of verification from your bank.

Biometric authentication



Authentication via SMS One-Time-Passcode



Please contact your card-issuing bank to get more information on the authentication method(s) they offer. If you have any other questions, check out our [FAQ](#) section or [contact us](#).



Sample copy 'Customer Information'

How does it work?

With Mastercard® Identity Check™ we leverage state-of-the-art technology to help your card-issuing bank check your identity when you make online payments with your Mastercard card at our shop.

This means all payments are checked in real time, with most approved by your bank instantly and 'invisibly', making your experience smooth and convenient.

No extra Authentication needed



When an extra layer of security is needed, at our checkout you will be asked to confirm the payment – for example by entering a one-time passcode (send via SMS) or using your fingerprint and your banking app or another familiar method of verification from your bank.

Biometric Authentication



Authentication via SMS One-Time-Passcode



Please contact your card issuing bank to get more information on the authentication method(s) they offer. If you have any other questions, check out our [FAQ](#) section or [contact us](#).

* NOT ALL AUTHENTICATION METHODS ALLOW TO ELIMINATE STATIC PASSWORDS. FOR EXAMPLE, OTP SMS MAY REQUIRE AN ADDITIONAL KNOWLEDGE FACTOR (LIKE PASSWORD, PIN OR SECURITY QUESTION) TO COMPLY WITH THE EBA REGULATORY TECHNICAL STANDARDS (RTS)

5 Help Page / FAQ – Introduction

As you have a website that deals with customers or the public in general there is bound to be a need for a support center including a comprehensive FAQ page. A great support center is where your customers can go to find answers to commonly asked questions and if it's done well it should be packed with useful information. If you set it up right and take the time to customise it, your support center can also be a seamless extension of your brand.

It is worth to put effort into making your support / FAQ page design as welcoming, clearcut, and as organized as possible so as to not overwhelm the reader.

In addition you might want to consider offering to search for answers by entering key words or ask questions with a live-chat functionality on your website. For some answers you'll be able to add value by offering actual step-by-step tutorials along with screenshots to help your customers figure out the steps they need to take to solve a problem or better understand a certain process. Again, think about breaking down the guidelines, e.g. by the type of device your customers are using.



Another essential part of every website is the “contact us” page. A well designed contact page directs people to the answers they need and helps them ask their questions more effectively, significantly improving their experience on your site – with the potential to reduce your customer service cost significantly.

But what constitutes a “well designed” contact page, and how do you know if you’re getting it right? Some of it is just trial and error, coupled with analytics from relevant tools that allow you to track user behaviour on your site.

But there are also best practices, like the following principles that can help building an effective contact page.

- **Help customers find the page:** Don't make people hunt for your contact page — stick with an obvious location.
- **Humanize your customer service team:** Use faces on your contact page
- **Centralize your contact options:** Use your contact page as a hub for all your support platforms, not just email.
- **Add structure to incoming questions:** The right amount of structure on your contact page can save time & hassle for you & your customers.
- **Set expectations for response times:** Don't make customers guess how long they'll wait for a reply - give them a timeframe on your contact page.

5 Help Page / FAQ – Introduction

Example: Cluster FAQs to help users find the answer faster



What is Mastercard® Identity Check™?



Why is the payment process changing?



How does Mastercard® Identity Check™ work?



How can I use Mastercard® Identity Check™?



Trouble Shooting



Search



Contact us

Do I need to register?
Do I need a new card?
Is it easy to use?
What happens if my card expires?
What if I use two cards?

Q: What is changing and what is Strong Customer Authentication (SCA)

A. The security rules of the new Payment Services Directive (PSD2) come into effect on 14 September 2019, introducing higher security standards for online payments that will help reduce online fraud. One mandatory component of PSD2 is the introduction of additional security checks – known as Strong Customer Authentication (SCA) - for online transactions. As a result, you will not be able to checkout online using just your card details, but will need to provide additional forms of authentication to validate the transaction and increase payment security.

By September 2019, all Payment Service Providers in the European Economic Area (EEA) are obliged to apply SCA, which means they have to request that their Cardholders use two different factors to verify payments. This is authentication based on the use of two or more elements categorised as “knowledge” (something only the user knows, e.g. a pass code), “possession” (something only the user possesses, e.g. a mobile device), and “inherence” (something the user is, e.g. a fingerprint).

Whereas today extra layers of authentication are the exception, additional authentication for online payments will become the new default after September 2019. Under certain exemptions to SCA the payment is approved ‘in the background’, without any Cardholder interaction, making your experience smooth and convenient.

The risk evaluation of each transaction is supported by an enhanced secured protocol called EMV® 3-D Secure (EMV 3DS), designed to improve your digital payment experience while reducing fraud, false declines and unnecessary friction. EMV 3DS is a global industry standard that helps to accurately verify Cardholders during online purchases, including recurring payments and credentials on file transactions. From 14 September 2019, the expectation is for all ecommerce transactions to be processed via EMV 3DS.

Q: What is Mastercard® Identity Check™ ?

A: Identity Check is Mastercard's new and improved payment authentication programme based on the global payment industry specification EMV® 3-D Secure, enabling greater security and a more user-friendly digital payment experience. Mastercard Identity Check leverages the updated EMV 3DS protocol to help reduce fraud and false declines of so called 'card-not-present transactions' – while providing you with a friction-free checkout experience whenever possible.

The new EMV 3-D Secure protocol comes with the power to exchange 10X more data between retailers and Issuers, e.g. for better authentication 'in the background', which adds to a smoother user experience and meets Strong Customer Authentication requirements under the European PSD2 regulation. It is applicable not only to browser based payments, but also mobile and in-app purchases. In many cases Mastercard Identity Check also helps eliminate static passwords for Strong Consumer Authentication (SCA) - based on the use of two or more elements - across all devices in real-time.

Q: How does Mastercard® Identity Check™ work?

A: Mastercard Identity Check leverages contextual data to deliver a user-friendly authentication standard that is supported by new European regulation. This means all payments are checked in real-time, and most are approved by your bank in the background, making your experience smooth and convenient.

When an extra layer of security is needed, at check-out you will be automatically prompted by your bank to provide additional information, e.g. your fingerprint or a one-time-password that is sent to your mobile phone or another familiar method of verification from your bank. Your identity is quickly confirmed by your financial institution and your purchase can be completed.

Q: What is EMV® 3-D Secure?

A: EMV 3DS is the new industry standard and protocol for retailers to send data to card Issuers during a so called 'card-not-present' transaction to help address false declines and lower card-not-present' fraud - while providing a better customer experience. EMV 3DS is relevant for all card-not-present' purchases, including recurring and card-on-file payments.

Q: What is Strong Customer Authentication (SCA) and how does it work?

A: Strong Customer Authentication (SCA) is a mandatory pillar of European PSD2 regulation, ensuring a high level of consumer protection and payments security. It will be required, e.g. when a consumer initiates an electronic payment transaction or carries out an action online that may imply a risk of payment fraud or other abuses. The regulation aims to address online fraud, by increasing the number of transactions subject to SCA.

To apply SCA, Issuers will request the Cardholder to provide two independent factors of validation by asking for a combination of two out of the three following categories:

- Something you know (e.g. PIN)
- Something you have (e.g. card/phone)
- Something you are (e.g. fingerprint)

This process is often referred to as 'two-factor authentication'.

SCA is applicable to all transactions where the card issuing bank and Acquirer are both based in the European Economic Area (EEA). The bank is responsible for the authentication of the Cardholder. PSD2 allows a number of exemptions to two-factor authentication, e.g. for payments below €30 or recurring payments of the same value. For more information, please see the separate section on PSD2 exemptions [ADD LINK].

Q: Does this mean that paying online with my debit or credit card was not safe previously? Why do we need a second authentication step now?

A: In the era of digitalization, customers and service providers cannot be too careful when it comes to preventing fraud; therefore, EEA members have decided to regulate electronic payments transactions. Mastercard and its partners are constantly developing safety and security solutions that evolve with prevailing law and industry provisions. Mastercard is committed to providing the best user experience possible and ensuring all transactions meet required standards and regulations.

Q: What exactly is meant by 'exemptions'?

A: PSD2 allows different 'exemptions to Strong Customer Authentication' - meaning that for those transactions no additional authentication is required. The objective is to optimise user experience by avoiding unnecessary friction.

Some of the most common exemptions are:

- A. Low value exemption
- B. Recurring payment exemption
- C. Merchant Initiated Transaction (MIT)* **including variable subscriptions**
- D. Whitelisting (or Trusted beneficiary) exemption
- E. Low risk transaction exemption (or Transaction Risk Assessment - TRA)

* Technically these payments are not an exemption, but fall outside the scope of SCA.

(...)

(...)

A. Low value exemption

Low value card transactions are those below €30 - they normally do not require Strong Customer Authentication (SCA). Strong Customer Authentication is required if the Cardholder initiates more than five consecutive low value payments or if the total payments value exceed €100.

B. Recurring payment exemption

Recurring payments of a fixed amount (such as subscriptions or membership fees) do not require Strong Customer Authentication (SCA), they will be exempt from the second transaction onwards. Only the initial transaction requires Strong Customer Authentication. If the amount changes, Strong Customer Authentication will be required for every new amount.

C. Merchant Initiated Transaction (MIT) including variable subscriptions

These payments are initiated by the Merchant without the interaction of the payer for each individual payment.

To set-up an MIT, SCA is required for the first transaction / action, as well as an agreement between Merchant and Cardholder specifying the reason for the payment and the payment amount (or an estimate when the precise amount is not known). Examples include:

- recurring transactions in which the value changes over time, e.g. for products or services that have a variable cost based on usage
- additional charges added to the initially agreed amount (mini-bar expenses, fines with a rental car etc.)
- the transaction is broken down into different payments happening at different times (e.g. instalments, travel bookings, market places).

(...)

(...)

D. Whitelisting / payments to trusted beneficiaries

This option means that a Cardholder can select certain retailers as 'trusted' and build a so called 'whitelist', which is governed by the Payment Services Provider (your bank). As a result, payments to these retailers won't require Strong Customer Authentication (SCA) in most cases. However, as a precondition at least one transaction must be validated using Strong Customer Authentication before the respective retailer can be added to the list.

It is important to note that it is the decision of the Payment Services Provider if the service is offered and if it's offered to all Cardholders or only those that are deemed to be below a certain fraud risk. The Payment Service Provider can still decide to request SCA if added security is needed, even if the retailer is on the whitelist of a specific Cardholder.

E. Low risk transaction exemption / Transaction Risk Analysis (TRA) exemption

This option takes into account that many transactions – after they have been evaluated in real time – are considered to be 'low risk' payments. This exemption has the widest extent and application, even though certain conditions are attached:

- A Payment Service Provider (e.g. an Acquirer) will act upon request of the retailer.
- + The Payment Service Provider has to prove a low fraud rate below a certain threshold.
- + The payment amount must fall under a certain threshold (less than € 500).
- + The Payment Service Provider holds the final authorisation decision and might still ask for Strong Customer Authentication (SCA) to validate the identity of the Cardholder.

Exemptions are not mandatory, meaning that Payment Service Providers (e.g. Issuers and Acquirers) may always choose to apply SCA.

Q: What made this kind of advanced authentication possible now?

A: Mastercard® Identity Check™ leverages a global industry standard called EMV® 3-D Secure to help reduce fraud and false declines of online transactions – while providing a frictionless checkout experience. EMV 3-D Secure is the enhanced version of an already existing ‘data flow’ designed to help retailers and Issuers authenticate so called ‘Card-Not-Present’ transactions. By exchanging some information between Issuers and retailers, it helps to accurately evaluate the transaction in real-time and verify consumers during digital purchases or other flows, such as recurring payments and card on file transactions.

Mastercard and the payments industry are implementing EMV 3-D Secure and raising the bar on authentication by enhancing security and simplifying the user experience across all digital channels. Reflecting consumer shopping habits, EMV 3-D Secure not only works for traditional web-browser/PC interfaces, but wherever Cardholders shop — on a mobile phone, tablet, or other smart devices or make app-based purchases.

Q: Do I need to register for Mastercard® Identity Check™?

A: Some financial institutions require you to sign up for their Mastercard Identity Check programme or accept updated Terms & Conditions – please speak to your bank to learn more about their specific offering.

We recommend you to check with your card issuing bank that you are fully set to use the new authentication standard that will be applied as of September 2019. If in doubt, please contact your financial institution to check if the details your bank has on file for you are up to date. For example: If your bank offers payment authentication via SMS one-time-password, they need your current mobile phone number to be able to send the code for each transaction.

Q: How does Mastercard® Identity Check™ protect me?

A: When making a purchase at a participating online retailer and you correctly verify your identity, you confirm that you are the authorised Cardholder - and your purchase will be completed. If incorrect details are entered, the purchase will not go through.

Q: Will I have to get a new card to use Mastercard® Identity Check™?

A: You will be able to use any of your existing Mastercard® credit or debit cards, as long as the cards are from a participating financial institution. However please speak to your financial institution about their individual authentication process and if any registration to the programme is needed.

Q: Is Mastercard® Identity Check™ easy to use?

A: Yes. As there are different ways to securely verify your identity to protect a purchase, please contact your card Issuer to learn more about their individual Mastercard Identity Check programme and how it works.

Please see the most common applications here [\[LINK TO USE CASES\]](#)

Q: What should I do if I don't know how to use the new authentication standard Mastercard® Identity Check™?

A: Contact the customer service number for your financial institution, which is typically found on the back of your card or at their website.

Q: How does this impact Mastercard® SecureCode™?

A: Current Mastercard SecureCode customers are requested to transition to Mastercard® Identity Check™ to take full advantage of the superior programme benefits. As the transition takes place, you will progressively see Identity Check information replacing SecureCode. Please contact your card issuing bank if there is any action needed from your side, in many instances the transition to Mastercard Identity Check will happen automatically.

Q: What if my authentication fails or I receive an error message?

A: To authenticate a payment, a Cardholder responds to a prompt from their bank and provides additional information. This may be something you know (e.g. PIN), something you use (e.g. card, phone), or something that's part of what you are (e.g. your fingerprint). If the payment authentication fails, you should contact the customer service number for your financial institution, which is typically found on the back of your card or at their website. Tell the customer service representative the message that you received.

Q: What if I did not receive an SMS/Text message with my one-time-passcode?

A: If your financial institution uses SMS/Text messages for authentications, you will need to contact the customer service number for your financial institution, which is typically found on the back of your card.

Q: What is the cost of the authentication SMS? Who pays this fee?

A: The SMS fee and its bearer is determined by the Issuer banks, just like in the case of regular notifications. Please check the Terms & Conditions of your bank with regards to this service.

Q: While staying abroad will I still receive an SMS for online authentication? Who will pay the fee for this?

A: You will still receive SMS for online authentication while you are abroad. The SMS fee and its bearer is determined by the Issuer banks, just like in the case of regular notifications. Please check the Terms & Conditions of your bank with regards to this service.

Q: What happens when my card expires?

A: You should receive a new card from your card Issuer and they will usually automatically update this information in your profile. However it might be needed to update your card number / credentials on file, if you use this service with selected retailers.

Q: What happens if I cancel my card and then get a new one with a different account number?

A: Please speak to your card Issuer with regards to the exact process which is also dependent on the services you use. For example, you might need to register the new card for their authentication programme or add your new card details to your wallet or update credentials on file with your favourite retailers.

Q: I would like to shop online but I don't have my mobile phone on me or the battery is low. How can I verify my identity?

A: If your verification method of choice depends on the usage of your mobile phone, then you will be unable to execute the Strong Customer Authentication at that moment and the payment procedure will fail.

Q: I use my debit/credit card to pay some bills online automatically every month. From now on will I have to verify my identity every time I pay?

A. Recurring payments do not need to be verified every time, no matter if the amount is the same or if it varies. Only the first payment - when setting up the regular payments - will require SCA to verify your identity and confirm the payments. You should also have an agreement between you and the retailer that specifies the reason for the payment and the payment amount (or an estimate when the precise amount is not known).

Q: I regularly shop at a specific retailer - will I have to verify my identity and payment every single time in the future?

A: It is up to the Issuer bank to decide whether to take advantage of the exemptions that PSD2 allows, e.g. offering Cardholders to build a 'whitelist' of trusted retailers where you do not always have to authenticate yourself. They might also decide to add individual rules around what retailers or products and services qualify for a 'whitelist' or if only payments below a certain threshold do not require additional authentication at whitelisted retailers.

Q: My phone doesn't have a fingerprint scanner, but does have a front camera. How can I verify my identity during mobile or contactless in-store payments?

A: In lieu of a fingerprint scanner, authentication of payments can be adjusted to other methods, such as screen lock, PIN code, and face recognition or in app authentication. This depends on the settings of your wallet and bank.

Q: I already have a Mastercard® Secure Code™-enabled card and I use one-time passwords received via SMS. What will change during my transactions?

A: Your bank might now offer other, more convenient means of identification, e.g. through their bank mobile application in combination with biometric authentication via fingerprint. Some might also continue to use a one-time password sent via SMS, most likely in combination with an additional identification factor in the form of a secret code or password to add a layer of security for your purchases. This is determined by the card Issuer and we recommend to check what could be the most convenient solution for your needs.

Q: I already have an online wallet/ my card is registered on a provider's website (e.g. PayPal or Simple). Will an additional verification step still be required?

A: Yes, since services like Simple or PayPal are subject to the Strong Customer Authentication requirements. The card Issuer will request that you authenticate when registering a new card for these services.

Q: How will the online retailer know that I'm registered for Mastercard® Identity Check™?

A: When you use a card that is enrolled in the Mastercard Identity Check programme at participating online retailers, the retailer automatically recognises your Mastercard at the time of the transaction.

Q: How will Mastercard® Identity Check™ change the online purchase process?

A: The online purchase process will change in the way that you will be prompted by your card issuing bank to provide some additional details to add an extra layer of security if needed. It is called ‘two-factor authentication’ or ‘strong customer authentication’ and can be done in many ways. For example, you may confirm your identity with a one-time password received in-app, via SMS or push, most likely in combination with an additional identification factor in the form of a secret code or password. Or you may confirm your identity by using the fingerprint scanner or other biometric technology with your smart phone and your bank’s mobile application. Your verification detail will never be revealed to the retailer during the checkout process. Ask your card Issuer about the authentication methods they offer.

Q: Will I be able to make purchases at retailers that accept Mastercard®, but do not participate in Mastercard® Identity Check™ ?

A: If you make a purchase at a retailer that does not participate in Mastercard Identity Check, you will not be asked for additional verification. You will continue to be protected from unauthorised purchases by [Zero Liability](#) [add LINK] from Mastercard.

Q: I have a card issued outside of EEA, but I would like to shop at an EEA web shop, what will I have to do?

A: EEA retailers are not obliged to support Strong Customer Authentication for cards issued outside the EEA region. However, the card issuing bank might support SCA by choice and still ask you to authenticate yourself.

Q: Will I be able to verify a digital card payment if I only have a smart watch or other smart wearable on me?

A: If the smart device in question is able to receive SMS (e.g. watch, bracelet, tablet etc.) or authenticate the Cardholder, verification will be possible and the purchase can be completed.

Q: If the bank provides options for both biometric and SMS code authentication, am I able to use both solutions for my online purchases?

A: If the card Issuer offers the option to choose from several solutions, you will be able to use the ones you chose for your online purchases

Q: How is Mastercard® Identity Check™ different from Zero Liability?

A: Using Mastercard Identity Check provides added security to prevent your card from unauthorised use. Exceptions apply. Zero Liability provides coverage if your card has been used fraudulently.

Q: Where can I view terms and conditions for the Mastercard® Identity Check™ programme?

A: Please visit your financial institution's website for the terms and conditions specific to your card.

Q: Where can I review the privacy policy for the Mastercard® Identity Check™ programme?

A: Please visit your financial institution's website to review the privacy policy specific to your card.

Q: Questions not answered here?

A: If your question is not listed, we recommend that you contact the financial institution that issued your account as only they hold information specific to your account. Typically, there is a customer service number for your financial institution on the back of the card.

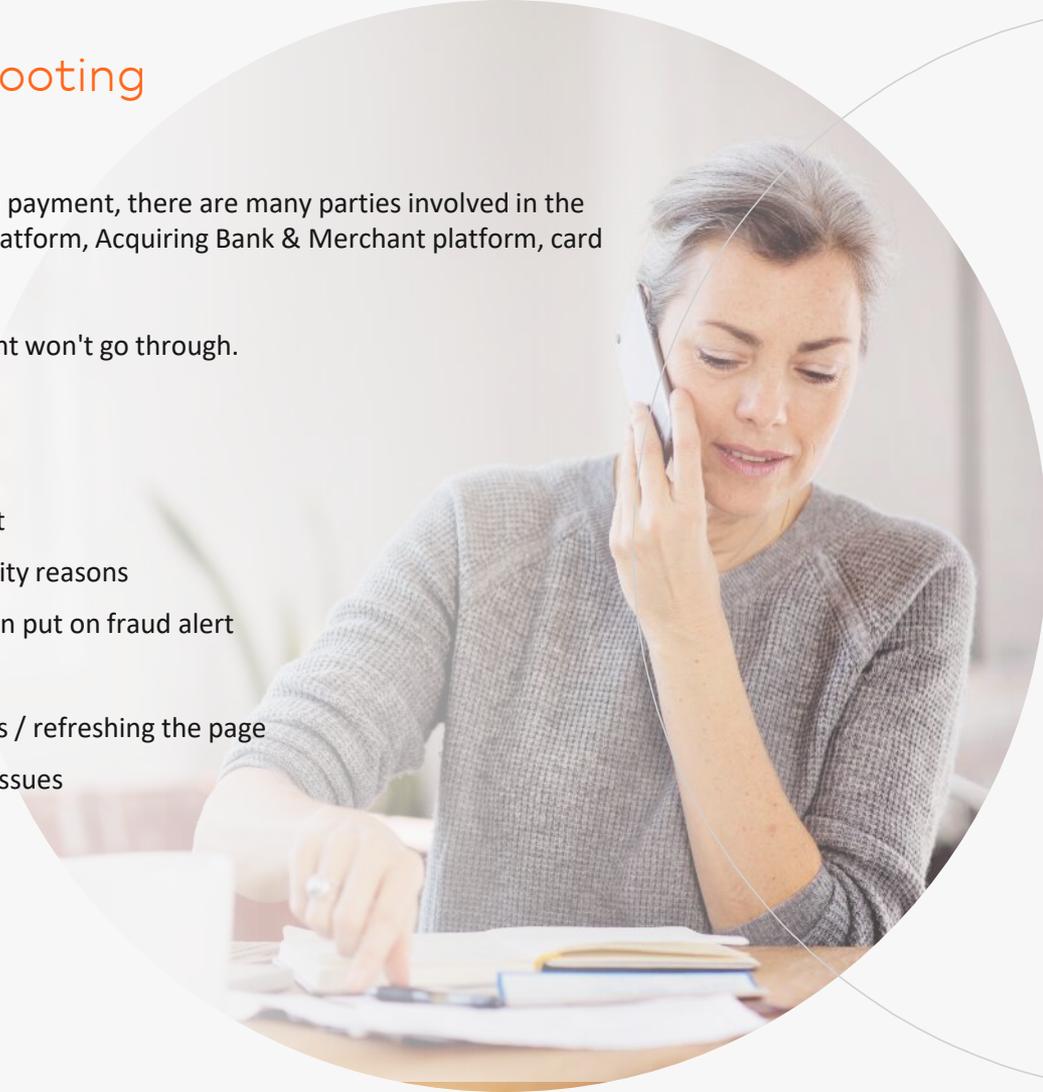
Q: Who do I contact for assistance with Mastercard® Identity Check™?

A: Please contact the financial institution that issued your Mastercard if you encounter any issues.

When a debit / credit card is used for making an online payment, there are many parties involved in the payment process: Issuing bank, Switches, Processing Platform, Acquiring Bank & Merchant platform, card networks and the Cardholders themselves.

There could be several different reasons why a payment won't go through.

- Card or other details are entered incorrectly
- Insufficient balance
- Card expired or new card hasn't been confirmed yet
- Card issuing bank declined the transaction for security reasons
- Card has been reported as lost / stolen or it has been put on fraud alert
- Account with the Merchant needs to be confirmed
- User dropped, e.g. because of time out, wrong clicks / refreshing the page
- Anti-virus, firewall software or connectivity / Wi-Fi issues
- Authentication failures



What message to display to Cardholders at checkout in case there is an authentication error?

In case of a failure during authentication the objective is to provide a clear messages to Cardholders offering guidance on how to solve the problem – and how to complete the purchase. As there may be different causes why a purchase cannot be completed the messages to the consumer need to be adjusted accordingly.

1. Failures during authentication:

- In this case usually the Issuer can solve the problem and an according note should be displayed to the customer. In EMV 3DS the Issuer can define a message such as “*Please contact us at the following number xxx-xxxxx or via email at customerservice@samplebank.com”*). It’s a so called free-form message triggered automatically within the authentication response message.

If the failure is not linked to the Issuer, but is due for example to a technical malfunction, we recommend using your existing error messages.

- If the customer still cannot complete the purchase, we recommend you initiate the usual basket abandonment process if technically possible (e.g. follow-up with the customer via SMS / Email, including the error message to help solve the issue). The message could be completed by recommending to use a different card / payment method to complete the purchase for now.

(...)

(...)

2. Failures during authorisation:

- Retailers should display an error message that reflects the decline reason code (and if provided, the Merchant advice code) provided by the Issuer. The message could be completed by recommending to retry or use a different card / payment method to complete the purchase for now.

There are a variety of other stumbling blocks that can interrupt the buying process or make it fail, such as technical errors, any kind of outage of the payments system, typical shopping cart abandonments, e.g. due to the checkout process itself, unexpected shipping costs or time etc. In those cases, we recommend you apply the usual processes you have put in place - including error messages to the customer.

No matter what the reason is for the purchase to fail, customer service increases the chance of salvaging the sale and maintaining a good relationship with the customer when they were ready to buy.

In case there are customer card payment issues beyond your control, consider displaying messages that help the Cardholder find a solution, for example:

“Your online payment security is very important to us. That is why you have been asked to authenticate your payment by providing additional information to your card issuing bank, so that they can approve the transaction. This additional information may be ‘something you know’ (like a password), ‘something you use’ (like your mobile phone), or ‘something you are’ (like your fingerprint).

For some reason the authentication failed this time – maybe try again or use a different card to complete your purchase. If the problem persists, we recommend to contact your card issuing bank, they can identify the problem and provide you with a solution. To protect your privacy, your card Issuer doesn't tell us why your card was declined.”

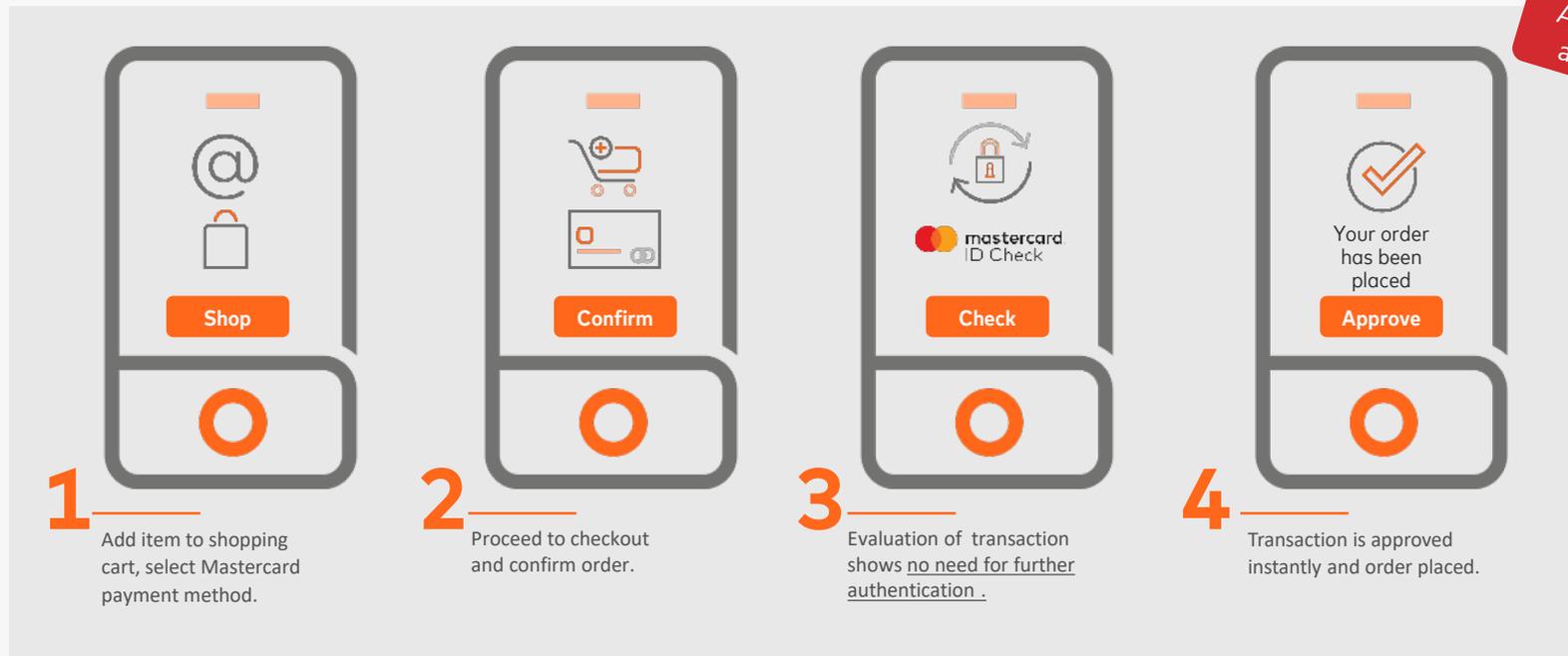
or

“If you know your card has been enabled for the Mastercard® Identity Check™ programme of your bank, but your payment still doesn't go through, we suggest that you try another card or try your transaction again later. Maybe contact your card Issuer to make sure you can complete your purchase without interruption next time.”

In addition, consider creating an alert for immediate notification when a customer's card is declined and contact them through a personalized email or by phone to offer assistance - offer some trouble shooting tips and if unsuccessful repeat the message to contact the card issuing bank.

Typical user journey (simplified): Frictionless checkout

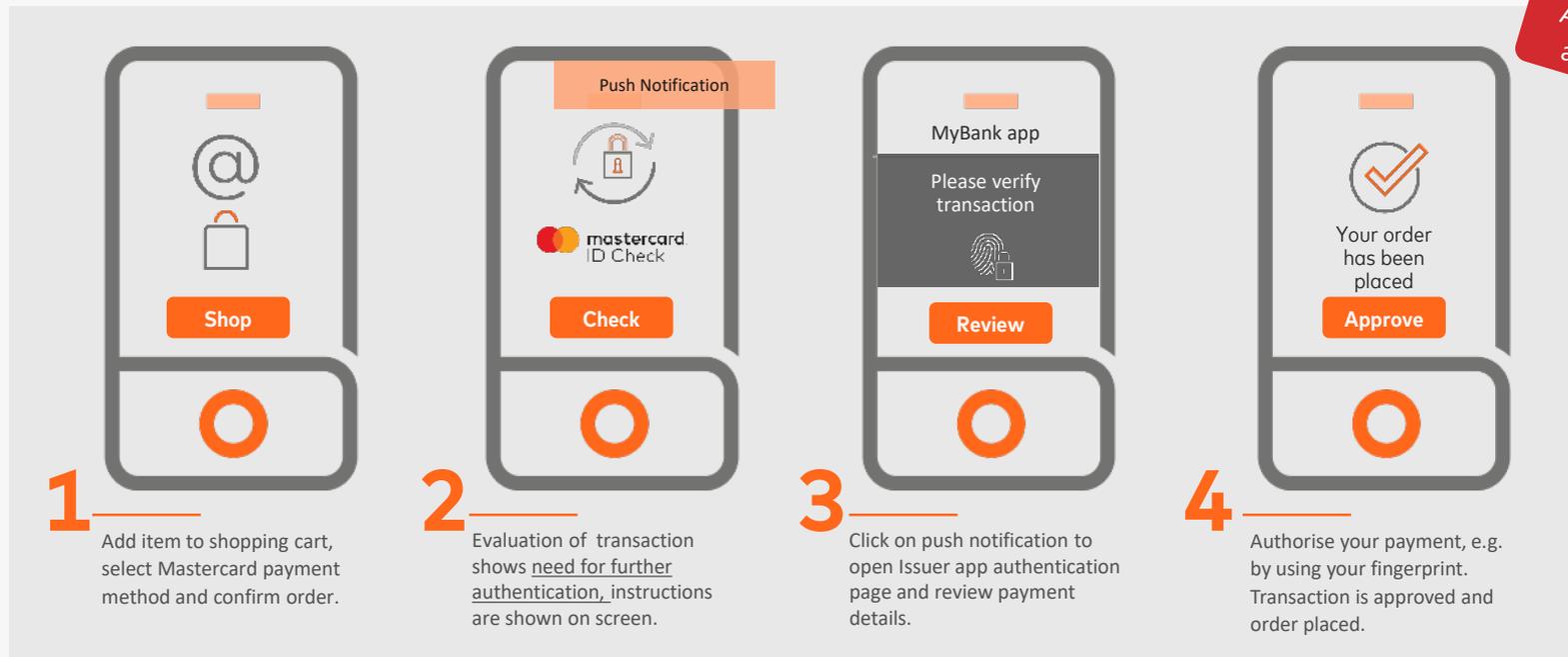
A frictionless checkout happens when the Cardholder is not challenged with an authentication request as a result of the Issuer assessment on the low risk of the transaction.



Pls. note: this is a simplified user journey, see “EMV® 3DS 2.1.0 / SCA User Experience Recommendations” for more details.

Typical user journey (simplified): Out of band / single device

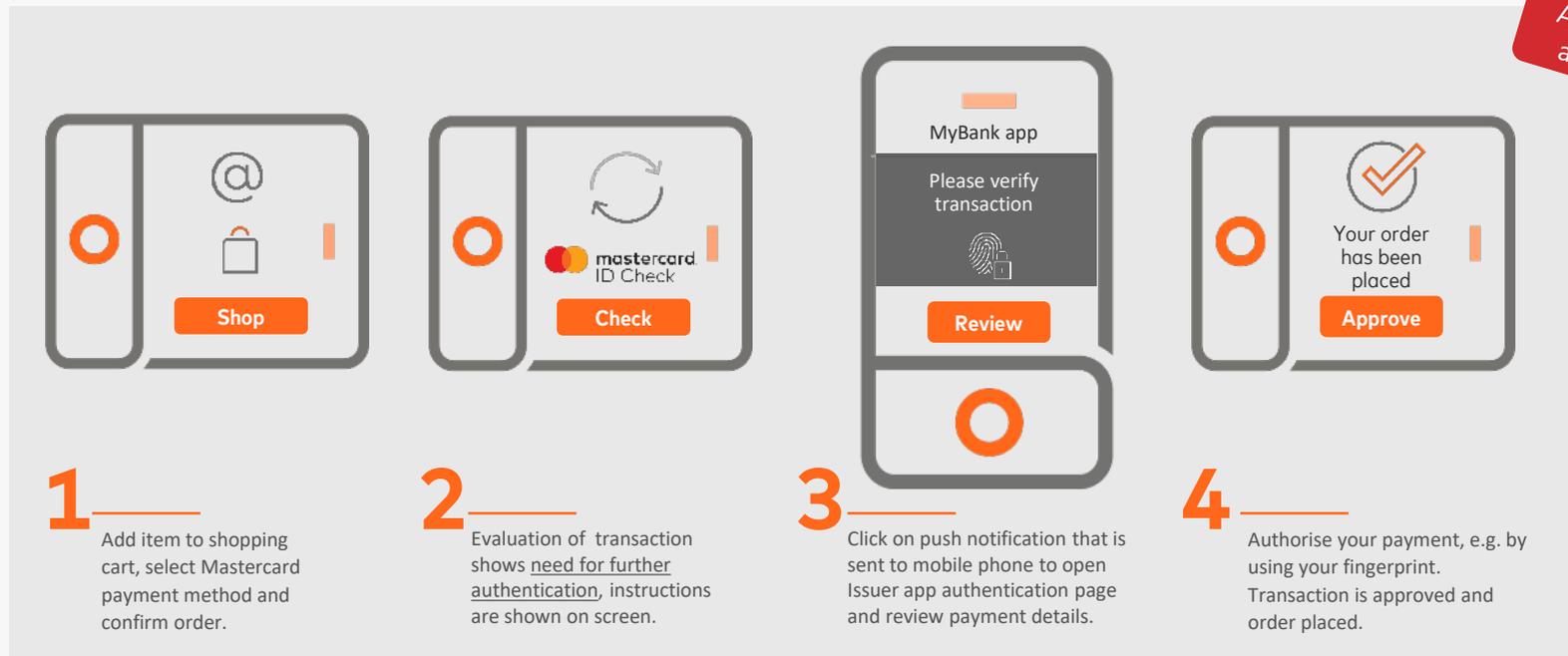
Out of Band (OOB) allows for Issuer authentication to occur outside the Merchant shopping environment, for example via push notification to a banking app. In this example one device (mobile phone) is used for both shopping and authentication.



Pls. note: this is a simplified user journey, see “EMV® 3DS 2.1.0 / SCA User Experience Recommendations” for more details.

Typical user journey (simplified): Out of band / multiple device

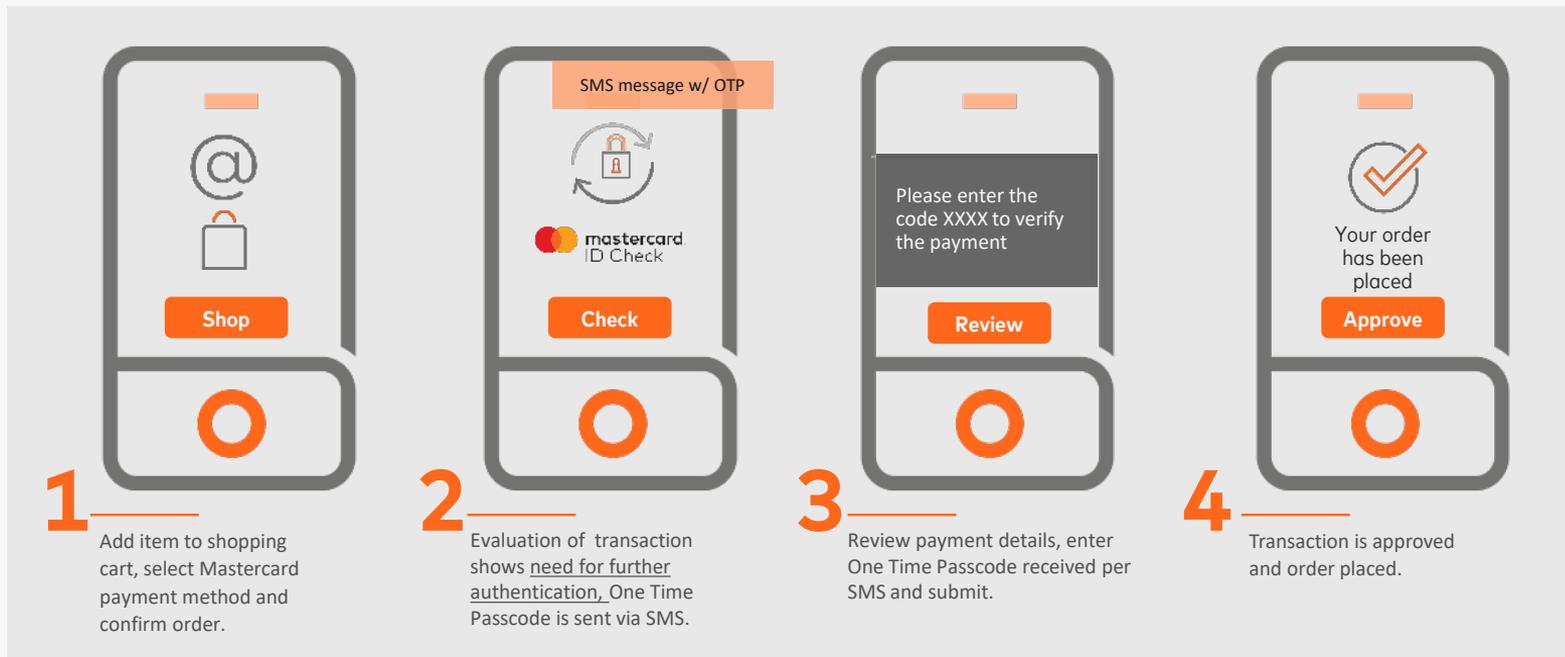
Out of Band (OOB) allows for Issuer authentication to occur outside the Merchant shopping environment, for example via push notification to a banking app. In this example different devices are used for shopping (tablet, laptop or PC) and authentication (mobile phone).



Pls. note: this is a simplified user journey, see “EMV® 3DS 2.1.0 / SCA User Experience Recommendations” for more details.

Typical user journey (simplified): One Time Passcode via SMS*

One Time Passcode (OTP) via SMS is one of the most commonly used methods for 3DS authentication in Europe today. However SCA compliance of this authentication method is currently under evaluation as the European Banking Authority (EBA) stated that card data was not considered a valid “knowledge” factor = together with OTP via SMS this would not be compliant with SCA. An additional authentication factor, for example a security question, would need to be added in the process. Please speak to your local C&I lead for more information on applicable practice in your market.



Pls. note: this is a simplified user journey, see “EMV® 3DS 2.1.0 / SCA User Experience Recommendations” for more details.



Mastercard Identity Check, an advanced solution to make your online payments simpler and safer, any time, across all your devices

- ...leverages contextual data to deliver a user-friendly authentication standard...
- ...payments are checked in real-time, and most are approved in the background, making your experience smooth and convenient.
- When an extra layer of security is needed, at check-out you will be asked to confirm your identity...

The toolkit contains editable files to allow customisation.

Please contact your Acquirer or Mastercard representative for source files and to discuss availability of translated copy.

General requirements

1. There are multiple configurations and versions of the Mastercard® Identity Check™ Product Mark. Use the correct one for your needs. Approved artwork may be downloaded from www.brand.mastercard.com (other marks).



General requirements (Cont.'d)

2. Always surround the Product Mark with sufficient free space, based on “x”, which is equal to the width of the “m” in the “mastercard” Logotype.

3. Always reproduce the Product Mark at a size that is clear and legible (depending on screen / print resolution).

Minimum free space

Minimum size

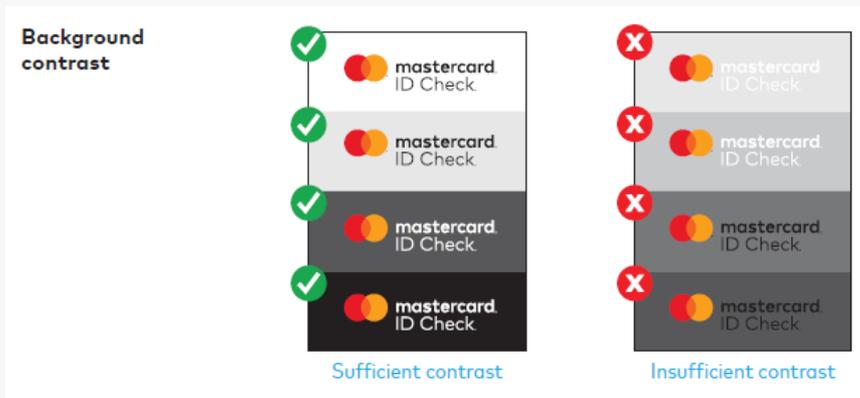
Screen: 45 pixels
Print: 16.8mm

Screen: 24 pixels
Print: 8.9mm

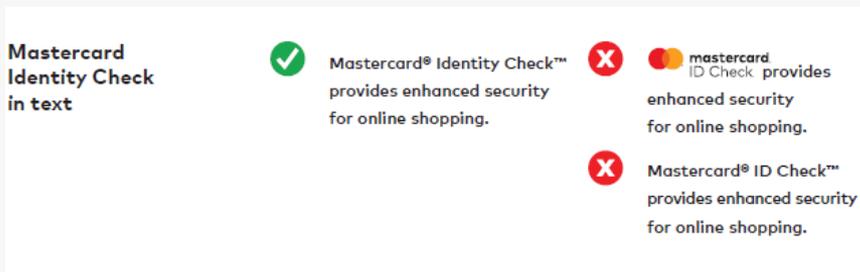
Screen: 70 pixels
Print: 25mm

General requirements (Cont.'d)

4. Always provide sufficient contrast with the background against which the Product Mark appears.



5. The Mastercard Identity Check Product Mark should be used in consumer-facing applications. For B2B materials, in text and verbally, the product should be referenced by its full name—Mastercard® Identity Check™.



If after reading the branding requirements you still haven't found the answer to your query, please contact us in one of two ways:
Email the Brand Manager ask.brand.manager@mastercard.com or call the Mastercard Brand Hotline 1-914-249-1326

Mastercard® Identity Check™ Branding Requirements – Use & Placement

Placement on a Merchant website

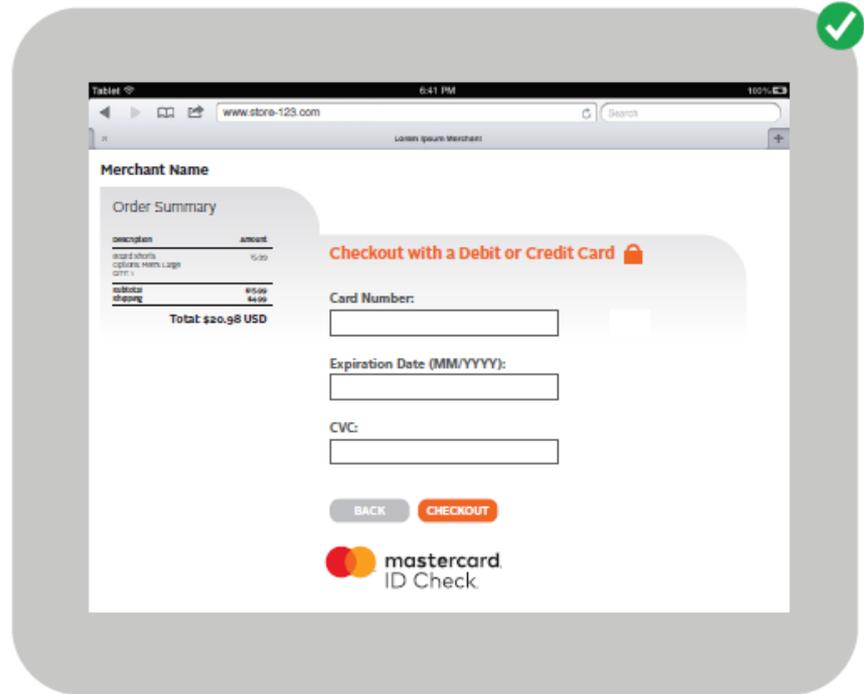
The Product Mark is provided to Merchants for display on their websites to indicate their participation in the Mastercard Identity Check programme. Use of the Product Mark by participating Merchants is mandatory.

It is recommended that the Product Mark appear on any page that displays payment options. Substantial free space between the Product Mark and the payment acceptance marks must be maintained.

In applications that promote more than one service brand, the Product Mark must be presented at parity in size, color, and frequency with all other brands.

Mastercard must review and approve all proposed use of the Product Mark on Merchant websites.

Recommended placement



The Product Mark represents the Mastercard® Identity Check™ service; it does not represent or replace the Mastercard Acceptance Mark on websites or other communications.

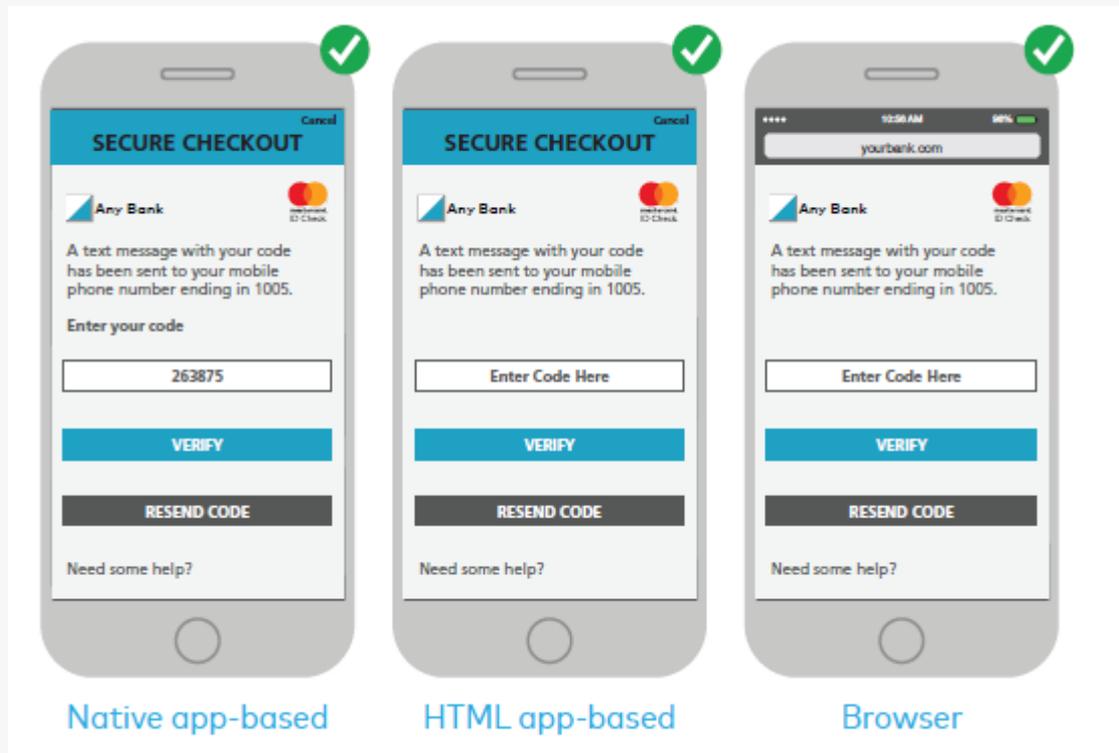
Mastercard® Identity Check™ Branding Requirements – Use & Placement

Placement within an Issuer portal

The Product Mark is available for customers or “on behalf of” application service providers to brand a Mastercard-sanctioned authentication programme. Use of the Product Mark is required for all such programmes and should appear in the Issuers’ enrollment screens and media as well as the purchase authentication window.

While Merchants may display multiple marks on their website, Issuer enrollment and authentication screens must not contain any other authentication product mark(s).

Recommended placement



Mastercard's brand positioning: Connecting people to Priceless possibilities

As a partner in delivering value to our customers and consumers, from marketing communications to product design, your support in aligning our brand identity across all the work you do with Mastercard will be critical.

WHAT WE CARE ABOUT



Inclusion

We believe in being a force for good where the underbanked benefit from the safety and convenience of our technology and network.



Innovation that matters

We believe in making dynamic connections grounded in human needs lead us to solutions that help business and consumers thrive.



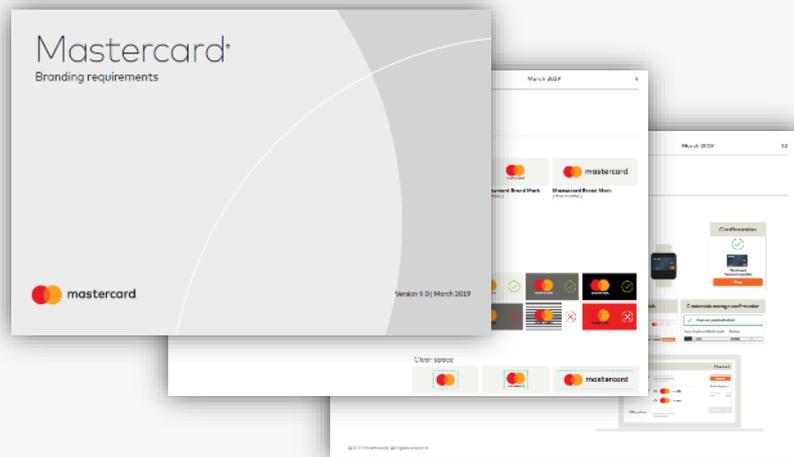
Safety in the world

We believe in continually advancing the security and integrity of our technology, products, and services so we can bring a peace of mind to all of our stakeholders, everywhere.



Enriching experiences

We believe that experiences matter more than things and will take every opportunity to enable services and experiences that enrich how we live.



Visit www.designcenter.mastercard and www.mastercardbrandcenter.com for more information



6. What's next



Get ready to reduce fraud and false declines of CNP transactions – with an enhanced check-out experience for cardholders

Mastercard will continue to engage in discussions with key players and stakeholders across the industry so that we can provide guidance and support to our customers to ensure the proper deployment of SCA. In summary, we recommend the following actions:

- Ensure compliance with PSD2 RTS (including Transaction Monitoring for fraud prevention) and Mastercard mandates
- Implement EMV® 3DS, ensure all necessary data is collected (e.g. via enhanced API) and provided in the authentication messages
- Register for EMV 3DS
- Leverage 3DS 1.0 where Issuers do not support EMV3DS 2.0
- Maximise the use of SCA Exemptions
- Consider Acquirer TRA exemption and review your fraud prevention strategy
- Adopt tokenisation for Credential on File
- Ensure you try again with 3DS authentication when your non-3DS authorizations are declined for non-financial reason
- Ensure authorization platforms can handle new data elements (that were announced by Mastercard and other schemes)
- Ensure fraud is reported to National Competent Authority (NCA) as per PSD2 RTS and EBA Fraud Reporting Guidelines

We encourage you to ensure that you have taken all the necessary steps to ensure delivery of the optimal customer experience. If you have any questions about SCA please contact your Acquirer, Gateway or Mastercard representative.



Legal note



Disclaimer

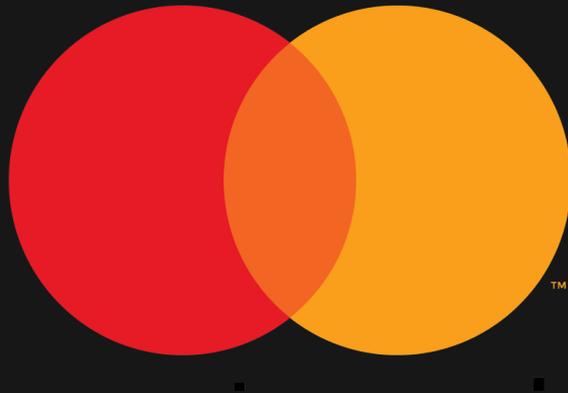
This document contains the proprietary and confidential information of Mastercard® Europe SA (“Mastercard”) and the information provided herein is strictly confidential. It is intended to be used internally within your organization and by receiving this information you agree that, except with the prior written permission of Mastercard, such information shall not be used for any unauthorised purpose and shall not be published or disclosed to third parties, in whole or part.

Information in this presentation or in any report or deliverable provided by Mastercard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates, or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both Mastercard’s and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent.

The information herein (also in the templates), including forecasts, projections, or indications of financial opportunities are provided to you on an “as is” basis for use at your own risk. Mastercard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation.

Mastercard makes no express or implied representations, warranties, assurances, or guarantees regarding: (i) the use of the information and templates; (ii) the accuracy, completeness of information contained herein; (iv) any intellectual property in or in connection with or arising from the creation, alteration, or use of the information and templates. Mastercard will not be responsible for any action you take as a result of using these templates or any inaccuracies, inconsistencies, errors, or omissions in the information and templates. Mastercard will not have any liability to you or any other person resulting from the use of such templates by you or any of your representatives.

This document and templates are designed to give an overview of the potential constructs and uses of Mastercard® Identity Check™. Local business, regulatory and legal considerations may restrict the availability or use of certain constructs referred to in the documents and you are fully responsible, without limitation, for identifying and taking into account all of the business, regulatory and legal considerations that may be relevant to your own business and the use of the templates..



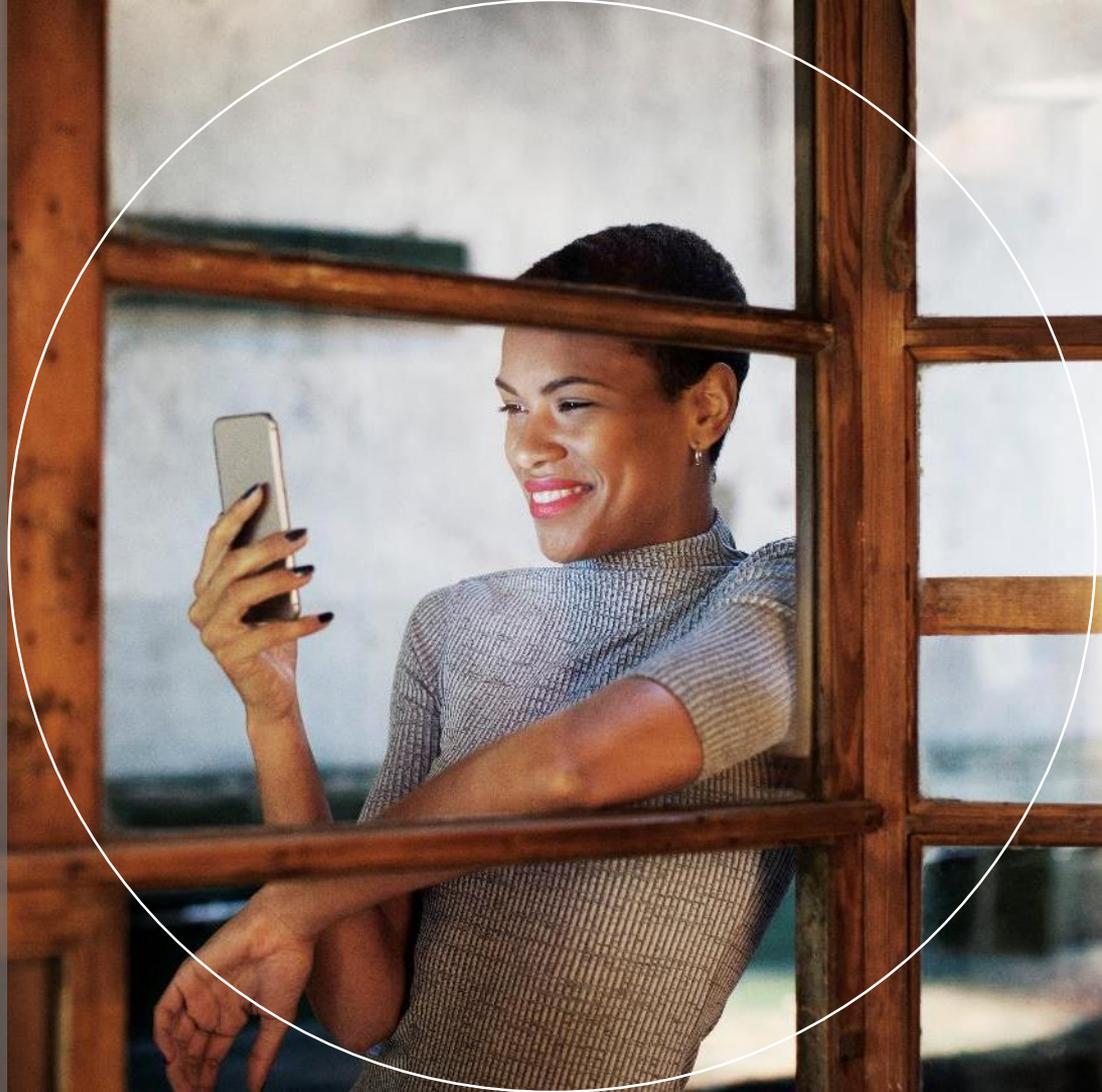
Mastercard is a registered trademark, and the circles design is a trademark of Mastercard International Incorporated.”



APPENDIX



Back to basics



What is PSD2, RTS and SCA?

Many of you will recognise terms such as PSD2, RTS and SCA but are you clear on what they actually mean? It's a complex topic and some may find it confusing and daunting and therefore have a tendency to push it to the back of their mind and forget about it.

However, this is not an option. Getting engaged may mean taking this back to basics, so here is a handy refresher on the key principles.

New standards & capabilities can drive security and enhance the user experience

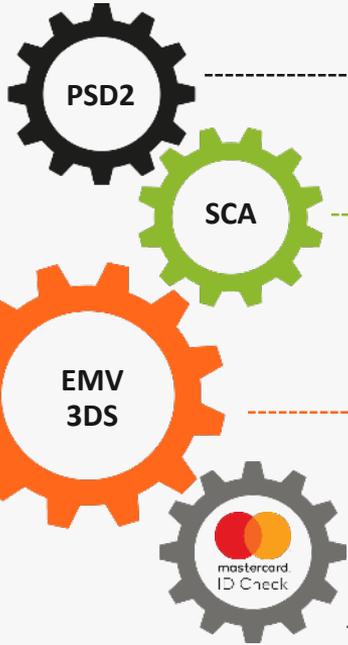
In a nutshell...

The **revised Payment Services Directive (PSD2)** aims to better align payment regulation with the evolution of the market and technology. It introduces (e.g.) higher security standards for online payments - this will make consumers more confident when buying online, but it'll also drastically impact the user experience.

Strong Customer Authentication (SCA) is a *mandatory* requirement for authenticating online payments that will be applied in Europe on 14 September 2019. It requires the use of two independent sources of validation = two of these three features: knowledge, possession and/or inherence - commonly known as 'two-factor authentication. To simplify life for consumers, there are a number of situations for which no SCA is required, most of these exemptions concern low-value payments, repetitive transactions (same amount) and transactions to trusted beneficiaries (white listing).

EMV® 3-D Secure (EMV 3DS) is a new global messaging protocol - a data flow - that helps enhance security and simplify the user experience across all digital channels (browser based, in app, wallets). It a) allows a frictionless authentication flow and b) enables consumers to authenticate themselves with their card Issuer when making online transactions, including COF or recurring payments.

Mastercard brands the technical standard EMV 3DS as **Mastercard® Identity Check™**. It leverages the EMV 3DS protocol with the power to exchange 10X more data between Merchants and Issuers, including new mobile capabilities. With this, Mastercard Identity Check helps improve digital payments security and increase approvals – while offering a frictionless payment experience to Cardholders whenever possible.



PSD2 requires that banks adjust security measures to the level of risk involved

- Mastercard® Identity Check™ helps improve digital payments security and increase approvals – while offering a frictionless payment experience
- The rich data exchange provided via EMV® 3-D Secure is used to determine the risk of a transaction and adapt security measures accordingly.

Frictionless flow



Intelligent friction



For those **transactions identified as low risk**, an Issuer can bypass any strong customer authentication (SCA) requirements, so that the payment can be **approved 'silently'** without any Cardholder interaction.

1 Risk based authentication is an exemption from SCA, it only applies if certain requirements are met, e.g. for transactions below €500 and if reference fraud rates are below a defined level.



Higher risk transactions can be prompted for **Cardholder authentication**, the Issuer then can insert 'intelligent friction' in multiple ways, e.g. Biometrics or One-time-password ², all meeting SCA requirements.

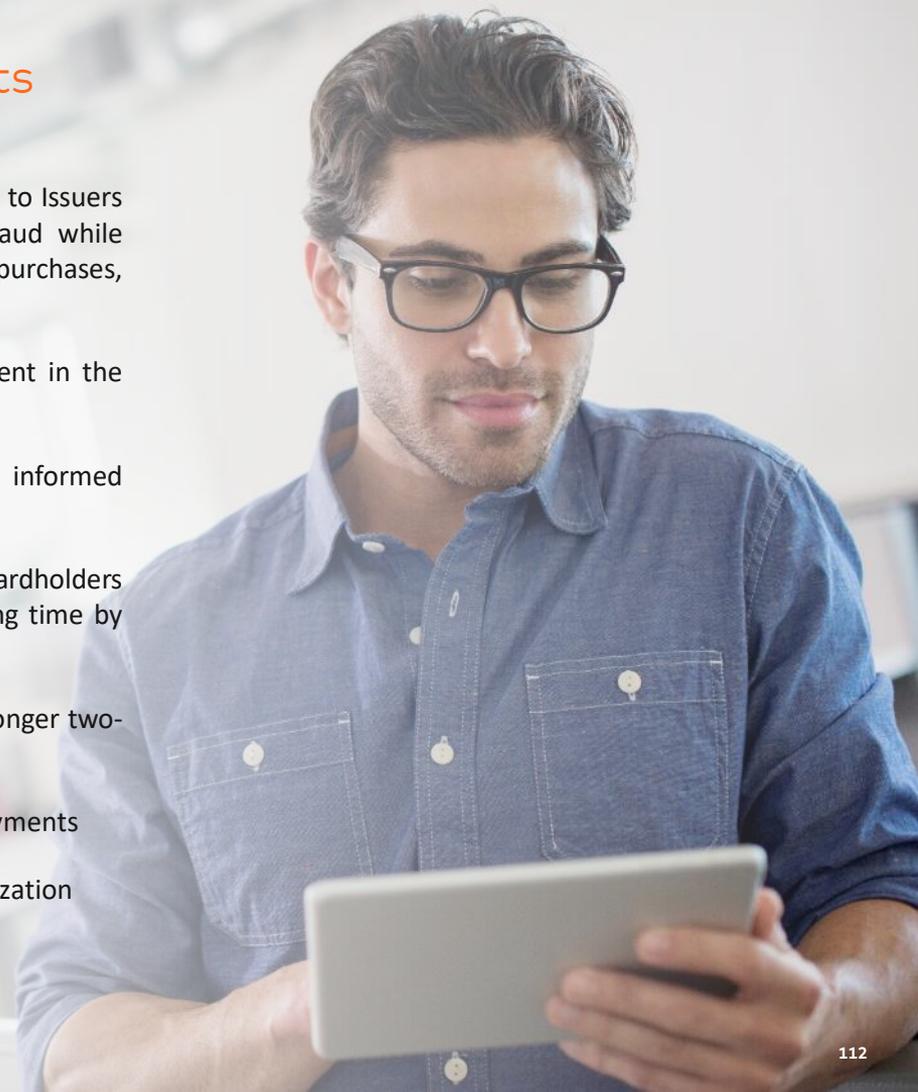
2 This may require an additional knowledge factor to comply with the EBA regulatory technical standards (RTS)

What is EMV® 3-D Secure and what are its benefits for the key stakeholders?

EMV 3DS is the new industry standard and protocol for Merchants to send data to Issuers during a CNP transaction to help address false declines and lower CNP fraud while providing a better customer experience. EMV 3DS is relevant for all CNP purchases, including recurring and card-on-file payments.

These new EMV 3DS standards improve on many of the shortcomings inherent in the original version. Some of these improvements include:

- ✓ Being able to exchange 10x more data than 3DS 1.0 to allow for more informed authentication and authorization decisions
- ✓ Performing risk-based authentication or frictionless authentication to allow Cardholders to be passively authenticated • Improving end-to-end transaction processing time by limiting the authentication cycle to one
- ✓ Enabling state-of-the-art authentication methods, such as biometrics, for stronger two-factor authentication
- ✓ Supporting new payment needs on any device, such as in-app and mobile payments
- ✓ Supporting additional use cases, for example, card on file, wallets, and tokenization
- ✓ Eliminating the need for consumer registration while shopping



What is Mastercard doing?

Launch of the Mastercard® Identity Check™

With the rollout of EMV® 3-D Secure, Mastercard has created a new solution called Mastercard Identity Check, which replaces Mastercard SecureCode that governed the old protocol.

Mastercard Identity Check leverages the updated EMV 3-D Secure protocol to help reduce fraud and false declines of card-not-present transactions – while providing Cardholders with a friction-free checkout experience.

This new solution will enable both Merchant and Issuer partners to take advantage of the new standards and capabilities to help drive simple and secure payments.



mastercard.
ID Check

EMV® 3-D Secure and Mastercard Identity Check provide the path to fast, frictionless authentication

Back to basics

What is PSD2?

The Second Payment Services Directive (PSD2) was officially published by the European Commission in December 2015, following on from the First Payment Services Directive (PSD1). Since the implementation of the PSD1 in 2009, the payments industry has undergone wide-ranging changes. Growth in ecommerce, increasing use of mobile devices for payments and increasing concerns regarding security provided some of the impetus to introduce further regulation, in the shape of PSD2. One of the key aims of PSD 2 is to reduce fraud. To this end PSD2 requires SCA for electronic payments.

What are the RTS?

The Regulatory Technical Standards on SCA and Common and Secure Communication (RTS) were published by the European Commission on November 27, 2017. They lay out the requirements for SCA. The RTS apply to browser-based payments, in-app and face-to-face payments, irrespective of device.

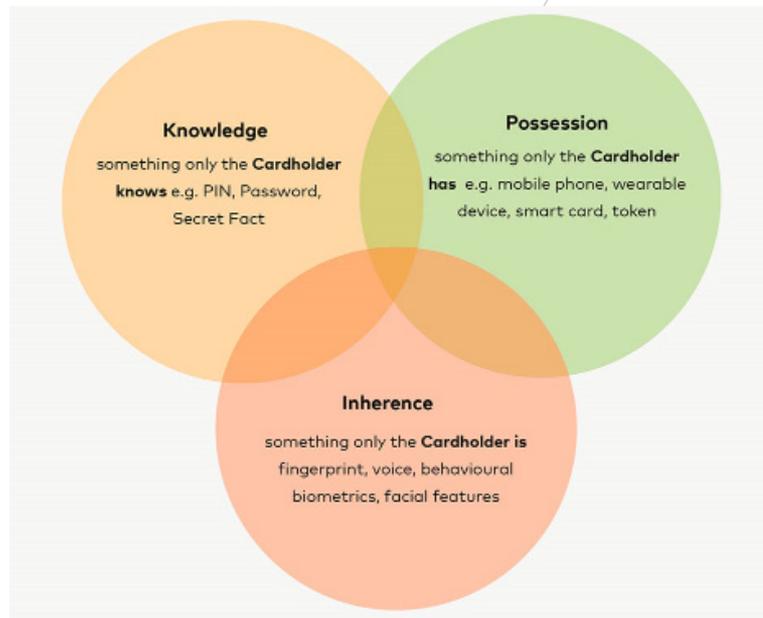
What is SCA?

SCA is an abbreviation for Strong Customer Authentication. The Oxford Dictionary defines “authentication” as the process or action of verifying the identity of a user or process. SCA is a set of requirements for authentication, defined by the European Banking Authority (EBA), and specifically introduces an extra level of security at the time of the payment transaction with the aim of reducing fraud through safer transactions.

Back to basics

What is Strong Customer Authentication (SCA), also called two factor authentication?

PSD2 requires that authentication must be “two factor”, that means it is performed using two sources of validation. They must be mutually independent, in that the breach of one does not compromise the reliability of the other. PSD2 requires that the two factors come from a choice of three different categories. These categories are as follows:



The use of a single device for authentication and shopping is expressly permitted, e.g. a smartphone may be used for both transacting and authenticating the Cardholder.

Back to basics

What are the most common SCA mechanisms in Europe?

The most common SCA mechanisms in the European region are:

- Authentication apps on mobile devices, often using Biometry – fingerprint, facial recognition on consumer devices (e.g. mobile phone)
- One Time Passwords (OTP) – sent via SMS*

When is SCA required?

SCA is mandated for electronic payments, including card payments from browser or in-app payments, on all devices. SCA should be applied where the payer:

- Accesses their payment account online, or
- Initiates an electronic payment transaction, or
- Carries out any action through a remote channel which may imply a risk of payment fraud or other abuses

Back to basics

The following are out of scope

- **Anonymous prepaid cards**

Anonymous prepaid cards by their nature as an anonymous payment instrument are not subject to the obligation of SCA. The Issuer will be the only one able to identify this type of card. The Acquirer will not be able to identify from the primary account number (PAN) that the product is anonymous.

- **Mail order / Telephone Order (MOTO)**

- **One Leg Transactions**

A one leg transaction is an expression which came about under PSD1 to refer to those payment transactions where the payer's or the recipient's PSP is based outside of the EU (indicating that the sender or the recipient is out of the EU).

- **Merchant Initiated Transactions (MIT)**

Examples of Merchant (or payee) initiated payments include magazine subscriptions, mobile phone bills and other agreements where a recurring sum is taken from the customer on a fixed date. These transactions of fixed or variable amount are initiated by the payee only without any direct intervention from the payer (= they are 'Merchant Initiated Transactions' or MITs). However, when the payer (Cardholder) sets up the initial mandate, this action requires SCA.

Back to basics

What is Dynamic Linking?

For remote transactions, each SCA must be linked to a specific amount and payee. This is called ‘dynamic linking’. This requirement, effectively binding authentication to the Merchant and amount, aims at ensuring that a valid authentication code is only used once and for the specific transaction for which the authentication is requested.

What is Transaction Monitoring?

The regulation mandates Transaction Monitoring for all transactions (Article 2 RTS). Transaction Monitoring is based on transaction information and allows building a risk score for each transaction. Transaction Monitoring and its associated risk scoring add value in both authentication and authorisation as they indicate the risk of the transaction. If risk scoring indicates that the transaction is risky, such transactions should be declined in authorisation, even when fully authenticated. An enhanced form of Transaction Monitoring is mandated for the application of the TRA exemption.

What are the key dates?

The PSD2 RTS requirements for SCA enter into force on 14th September, 2019. Mastercard has published a number of announcements regarding key dates on the road to implementing SCA. You can find the key dates outlined in “Mastercard’s Authentication Guide for Europe”.

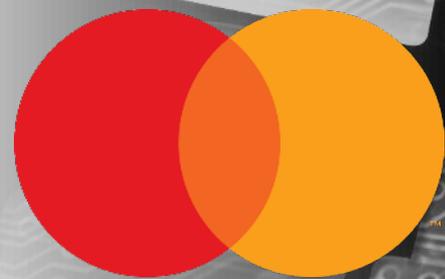


Mastercard® Identity Check™



Mastercard® Identity Check™ helps improve digital payment security and increase approvals – while offering a frictionless payment experience to Cardholders

- ✓ Mastercard Identity Check is a next generation authentication solution that enables greater security and a user-friendly digital payment experience.
- ✓ It helps reduce fraud, false declines and unnecessary friction - while meeting Strong Customer Authentication (SCA) requirements under the PSD2 regulation.
- ✓ Mastercard Identity Check leverages the new EMV® 3-D Secure protocol with the power to exchange 10X more data between Merchants and Issuers, including new mobile capabilities – raising the bar on authentication.



mastercard
ID Check

The new EMV® 3-D Secure standard allows to drive greater security and profitability –while enhancing the user experience (UX) for all Cardholders

	3DS 1 Standards	NEW EMV 3DS Standards
METHOD	Static passwords/ security questions	Eliminates static pass-words for stronger two-factor authentication
INTERFACES	Browser dependent	Supports new payment needs, such as in-app and mobile payments
DATA	Only 15 data elements available	Enables 10X more data to be exchanged
USE CASES	Supports guest check-out only	Supports additional use cases , e.g. Card on File, wallets, tokenization, etc.
DECISIONING	Merchants bound by Issuer decisioning	Enhances decisioning by increased Merchant flow of data

Benefits of NEW EMV 3DS
<ul style="list-style-type: none"> • Greater security • Greater convenience
<ul style="list-style-type: none"> • Better UX • Wider applications
<ul style="list-style-type: none"> • Improved decisioning
<ul style="list-style-type: none"> • Expanded use • Greater security
<ul style="list-style-type: none"> • Greater flexibility

Mastercard® Identity Check™ builds upon the enhanced EMV® 3DS protocol to address digital payment changes and challenges

Secure Code

(based on 3DS1 Standards)

MasterCard
SecureCode™

Multiple authentication methods



- Web only
- Limited data
- Payments only

Mastercard Identity Check

(based on NEW EMV 3DS Standards,
replaces Secure Code)

 **mastercard**
ID Check

Biometric-based authentication



with SMS OTP + 1 factor as back-up

- **Multiple channels** (web and mobile App)
- **Much more data and options** (to better manage the risk)
- **Payments and beyond**

EMV® 3-D Secure and Mastercard® Identity Check™ offer clear benefits to all stakeholders



Eliminates static passwords for **Strong Consumer Authentication (SCA)** - based on the use of two or more elements - across all devices in real-time

Supports new payment needs, like authorization via mobile devices or in-app payments

Delivers a **better online payment experience for consumers...**

...by **reducing Cardholder verification needs**: risk-based authentication (RBA) allows most transactions to be approved directly and without Cardholder interaction, only challenging higher-risk transactions to be validated using SCA

...by offering simple and intuitive options for **consumers to verify their identity if needed**, supporting biometrics, dynamic passwords, security questions, plus proprietary options

...by **driving frictionless alternatives**, like Credentials-On-File (COF) or Whitelisting, as a result of connecting Issuers and Merchants to drive data exchange

Can be **seamlessly integrated** into the Merchant's checkout process

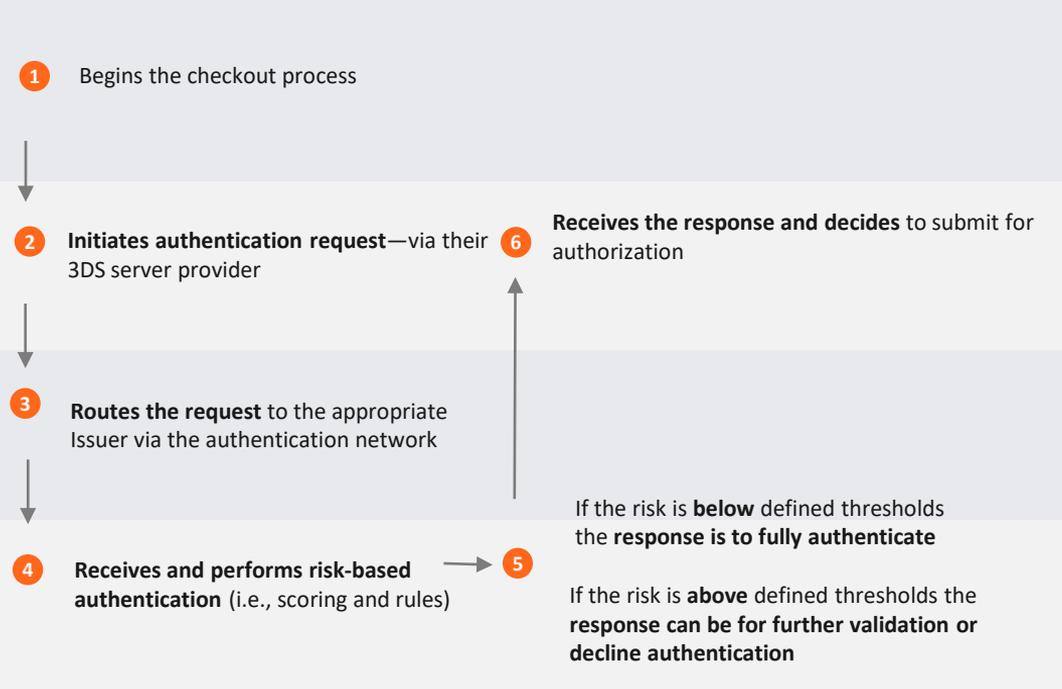
Offers the flexibility to address enhanced Issuers needs, such as **securing banking applications, out-of-band authentication**, etc.

Merchants and Issuers participate in EMV® 3DS via third party service providers with Mastercard as the connecting link



Mastercard® Identity Check™ seamlessly integrates into the transaction flow to deliver secure authentication

With Identity Check & EMV® 3DS



Consumers now can easily prove their identity, if needed with dynamic passwords or biometrics

Merchants have greater ability to share information with Issuer to help improve risk models

Issuers/ACS providers now can receive 10X more data to help them make more informed decisions

Mastercard[®] Identity Check[™] is simple and easy for Cardholders to use

If the Cardholder is required to authenticate themselves at checkout, the Issuer can insert intelligent friction in multiple ways



EMV[®] 3-D Secure Transaction Authentication

Frictionless Flow Majority of transactions



Risk Based Authentication (RBA)

Risk Based Authentication utilizes the rich data exchange provided via EMV 3-D Secure to determine risk.

Transactions deemed low risk may be silently authenticated without unnecessary friction—while higher risk transactions can be prompted for Cardholder authentication resulting in:

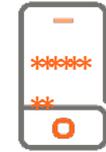
- Vast majority of Cardholder experiences are seamless with no friction
- “Silent” authentication happens in the background, without the consumer awareness of the process after they initiate payment

Intelligent Friction Minority of transactions



Biometrics

- The Cardholder is prompted to authenticate on mobile device
- Authenticates with pre-selected biometric method: fingerprint, face, voice, other.



One Time Password

(fallback solution)*

- Cardholder receives a one-time use code through the mobile banking app or via SMS text message from Issuer
- Enters code on the authentication page and is verified as correct

* THIS MAY REQUIRE AN ADDITIONAL KNOWLEDGE FACTORY TO COMPLY WITH THE EBA REGULATORY TECHNICAL STANDARDS (RTS)

In summary: Mastercard® Identity Check™ meets the need for simple and secure payments and helps everyone 'win' from EMV® 3DS and PSD2

Consumers



- **Eliminates the frustration** of managing and remembering passwords
- Provides strong **protection** for financial data
- **Minimizes disruptions** due to decrease in fraud by 50% (fully authenticated vs. 'Merchant only' transactions³)

Merchants



- **Helps drive revenue** by reducing cart abandonment of up to 70% when biometric identification is used¹
- Hassle-free authentication can help Merchants **gain greater share** in their category
- Authenticated transactions have **higher approval rates of +10pp²**

Financial Institutions



- **Decreases fraud** by eliminating the risk from passwords
- Enhances Cardholder **engagement** and loyalty⁴
- Increases revenues via **increased completed transactions**
- **Lower customer service costs** due to fewer calls and password resets

In addition: Mastercard® Identity Check™ offers a mobile biometric solution to secure digital payments and mobile banking applications



App-based hosted solution leveraging the mobile device to secure online payments and mobile banking applications

Comprised of two main components

- 1 Front-end biometric **app** that supports both fingerprint and facial recognition
- 2 Back-end biometric **authentication platform**

Plug and Play Deployment models through our SDK

Software Development Kit (SDK) for Issuer's Mobile Apps
Integrated into Issuer app; used for mobile banking, call center, suspicious transactions and digital payments

Biometric authenticators available

- Fingerprint (Touch ID, Android Finger)
- Facial recognition
- Face ID
- Voice recognition
- Samsung Iris
- Passive Biometrics (NuData)



How we help



How Mastercard drives the process

Mastercard is actively engaged in discussions with key players and stakeholders across the industry and is investing both time and resources to provide guidance and support to our customers. In so doing, our aim is to ensure the proper deployment of SCA so that together we can deliver the optimal customer experience.

We are doing this in a number of ways:

a. Addressing ambiguity

There are still a number of points that are unclear and require further clarification. Mastercard continues to engage with the EBA to raise questions on the interpretation of RTS on Strong Customer Authentication and Common and Secure Open Standards of Communication. As responses are published these will be reviewed and incorporated as appropriate into future documentation, rules and guidance.

Speak to your Acquirer or Mastercard representative for more information regarding questions to the EBA on the interpretation of RTS.

How Mastercard drives the process

b. Creating consistency

At Mastercard we work to create standards that enable worldwide interoperability & security. Through our participation in various industry groups and organisations we strive to bring about greater consistency. Some of the groups in which we are involved include the European Cards Stakeholders Group, NEXO, EMVCo and the European Payments Council. Perhaps of most importance for consistency is EMVCo. EMVCo has published standards on a number of topics including contact and contactless cards, QR Codes and EMV 3DS 2.0.

As a founding member of EMVCo, Mastercard has been heavily involved in the evolution of the current authentication interface (3DS 1.0) into EMV 3DS 2.0, an industry standard that underpins SCA and:

Enables the exchange of more transaction and consumer data, enhancing the Issuer's decision making and allowing them to determine when SCA exemptions apply Supports new payment needs, such as in-app and mobile payments Supports additional use cases, such as Credential on File, Wallets and Tokenisation The new standards became operational on 6 November 2018. They are published on the [EMVCo website](#).

How Mastercard drives the process

c. Updating Rules

Mastercard is changing its rules to support the application of SCA. These changes are published in our Announcements on MC Connect (access for Acquirers).

Examples include: Changes to accommodate new flags and data fields in both authentication and authorisation messages Changes to facilitate the use of exemptions Introduction of new reason codes to address Issuer declines for no 3DS transactions.

How Mastercard drives the process

d. Products and Solutions

Mastercard® Identity Check™

Mastercard Identity Check is the new programme and brand for Mastercard authentications based on the EMV® 3DS standard. It replaces the former SecureCode brand and previous 3DS version as of April/December 2019 (depending on the country) and provides a seamless authentication experience across payment environments and devices. With EMV 3DS and Identify Check, ecommerce Merchants will be able to achieve the same performance levels as bricks and mortar store Merchants (using Chip and PIN, as measured on the Mastercard network).

Mastercard Authentication Risk Model

Mastercard is leveraging its authentication and authorisation network intelligence and will be adding our risk score to the EMV 3DS authentication responses to help Acquirers comply with the Transaction Monitoring requirement under PSD2. Combining the incremental EMV 3DS data with Mastercard fraud data authorisation intelligence means that we can also provide Issuers with insights that will help them to make better risk based decisions and offering greater confidence in their decisions. As a result Acquirers should expect to see higher levels of approvals, increasing Merchant sales and growing revenue.

How Mastercard drives the process

e. Sharing insight

There is a myriad of information available on the topic of PSD2 RTS and SCA. Speak to your account manager to get access to the range of materials produced by Mastercard (listed in alphabetical order), most documents are also available in Mastercard Connect.

- **3DS 2.0 UX Recommendations**

- **Mastercard Academy webinars**

Mastercard Academy offers several webinars related to EMV® 3DS, the Mastercard® Identity Check™ Programme and PSD2 RTS SCA Requirements.

- **Mastercard Authentication Guide for Europe**

This document has been prepared to provide all stakeholders involved directly or indirectly in the authentication value chain with elements to understand and start preparing for the roll-out of EMV 3DS (3DS 2.0) and the Mastercard Identity Check Programme. It complements the Mastercard Identity Check Global Programme Guide. The Guide is updated regularly the next edition has just been published in March.

- **Mastercard Identity Check Global Programme Guide**

- **Mastercard Standards for Merchant White Listing**

- **Mastercard Summary of liability for fraud under SCA**

(...)

How Mastercard drives the process

(...)

- **Strong Customer Authentication and Merchant Initiated Transactions**

This is a position paper outlining Mastercard's view on the scope of Merchant Initiated Transactions and its application to card payments.

- **Strong Customer Authentication and PSD2 – How to adapt to new regulation in Europe**

published Aug 2018

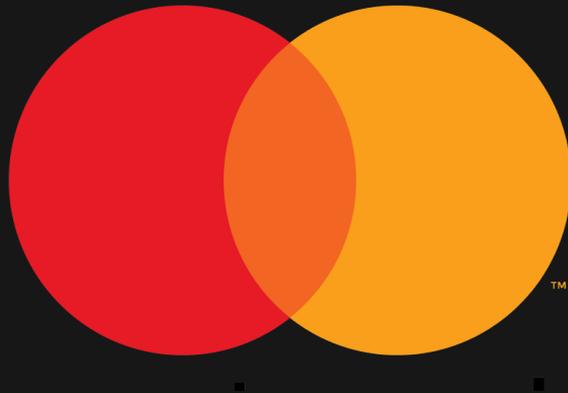
This is a comprehensive overview of the new regulatory requirements for SCA, Mastercard's Authorisation Strategy and the key decisions that both Acquirers and Issuers need to take.

- **Strong Customer Authentication Card and EMV® 3DS data**

- **Useful Websites**

- [EBA PSD2 RTS](http://www.eba.europa.eu) (www.eba.europa.eu)

- [EMVCO 3D-Secure Specifications](http://www.emvco.com/emv-technologies/3d-secure/) (www.emvco.com/emv-technologies/3d-secure/)



Mastercard is a registered trademark, and the circles design is a trademark of Mastercard International Incorporated.”