mastercard

Strong Customer Authentication and PSD2

How to adapt to new regulation in Europe

January 18, 2018

Authors:
Christoph Baert
Paul Baker

1. INTRODUCTION 3

2. WHAT IS MASTERCARD'S AUTHENTICATION STRATEGY IN EUROPE? 3

SEAMLESS SCA FOR HIGHER CONVERSION AND APPROVAL RATES 4
RISK-SCORING FOR SECURITY AND ONE-CLICK PAYMENTS 4
RULES CHANGES TO FACILITATE USE OF EXEMPTIONS 5
FINALIZATION OF MASTERCARD'S AUTHENTICATION INFRASTRUCTURE 6
PUBLICATION OF SAFETY & SECURITY ANNOUNCEMENTS 6

3. THE NEW REGULATORY REQUIREMENTS FOR SCA 6

WHAT IS SCA? 6
WHAT IS DYNAMIC LINKING? 7
WHEN WILL SCA APPLY? 7
WHICH TRANSACTIONS ARE EXEMPTED FROM SCA? 8
WHITE-LISTS OF TRUSTED BENEFICIARIES. WHAT IS WHITE LISTING? 8
WHAT IS THE TRA EXEMPTION? 8
HOW ARE RECURRING TRANSACTIONS IMPACTED? 10
CARD ON FILE MERCHANTS. ARE THERE EXEMPTIONS AVAILABLE? 10
HOW DOES THE EXEMPTION FOR LOW-VALUE REMOTE PAYMENTS WORK? 10
WHAT IS THE IMPACT ON CONTACTLESS PAYMENTS? 10
WHICH EXEMPTION WILL COMMERCIAL CARDS BENEFIT FROM? 11
WHAT IS THE EXEMPTION APPLICABLE TO UNATTENDED TERMINALS FOR TRANSIT AND PARKING? 12
WHAT IS TRANSACTION MONITORING? 12
IS CARD DATA A VALID AUTHENTICATION FACTOR? 12
IS DELEGATED AUTHENTICATION TO A SMARTPHONE ALLOWED? 12
IS DELEGATED AUTHENTICATION TO A MERCHANT ALLOWED? 12
IS PERSISTENT AUTHENTICATION FOR WEARABLE DEVICES ALLOWED? 13
HOW WILL THE EXEMPTIONS' EURO LIMITS APPLY FOR TRANSACTIONS IN OTHER CURRENCIES? 13

4. WHAT ARE THE KEY DECISIONS I NEED TO MAKE AS AN ISSUER? 13

BIOMETRIC AUTHENTICATION 13
WHITE-LISTING 14
TRANSACTION RISK ANALYSIS (TRA) EXEMPTION 15
OTHER EXEMPTIONS 15
CARD ON FILE 15
CVM DELEGATION 15

5. WHAT ARE THE KEY DECISIONS THAT I SHOULD MAKE AS AN ACQUIRER? 16

WHITE-LISTING 16
RISK-SCORING 16
TRA EXEMPTION 16
CARD ON FILE 16

6. CONCLUSIONS 16

1. Introduction

New regulatory requirements on strong customer authentication (SCA) will make authentication a key focus for customers in Europe. While this document is addressed to Issuers and Acquirers, the new requirements will also have an impact on merchants and cardholders, as well as other players in the payment ecosystem (e.g., wallet providers, Access Control Server (ACS) and other technical service providers).

The new requirements are contained in the Revised Payment Services Directive (PSD2) and in the Regulatory Technical Standards on SCA and Common and Secure Communication under PSD2 (RTS), which the European Commission published on November 27, 2017.

PSD2 aims to reduce fraud in electronic payments. It mandates SCA for electronic payments, including card payments. The RTS detail the SCA requirements and set out the exemptions from SCA.

Past regulation was restricted to browser-based payments (EBA Guidelines on the security of internet payments). The scope of the regulation is now extended to in-app and face-to-face payments. All devices are covered (e.g., desktop, mobile, wearable devices and Internet of Things (IoT)).

The PSD2 SCA requirements will apply in 2019 (18 months after publication of the RTS in the Official Journal of the European Union). The regulation will apply in all the Member States of the European Union and in Iceland, Lichtenstein and Norway.

2. 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 with 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 from SCA.
   This can be achieved with changes in our rules that facilitate the application of the exemptions and a shift in liability.

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 and payment experience for cardholders across payment environments and devices (face-to-face and e-commerce, in-app and within websites, IoT). Mastercard Identity Check implements the EMVCo 3DS 2 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).

Mastercard is mandating that Issuers offer their customers biometric authentication for Mastercard Identity Check/SecureCode and Masterpass transactions, including NFC mobile transactions. Issuers will have to offer an alternative authentication method for cardholders without a smartphone (e.g., an OTP via SMS).

SCA must be based over time on non-static authentication (see Security Bulletin on Identity Check published in October 2016).

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. This layered approach (or defence in depth) provides much greater protection for all parties than the reliance on a single-layered approach, no matter how strong that approach or authentication may be.

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 possible under the new regulation.

In order to achieve a complete risk-scoring for each transaction, 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. Merchants can also provide this information to the Acquirer to enable the Acquirer to apply the TRA exemption.

In the Mastercard network, Acquirers will not be liable for fraudulent transactions when merchants initiate an authentication request using the EMVCo 3DS 2.0 flow (Mastercard Identity Check). An exception to this rule is that when the Acquirer applies the TRA exemption, the Acquirer will be liable. Mastercard is requiring that merchants support EMVCo 3DS 2.0 (or an alternative technological SCA solution) in all European countries (except Switzerland).

Mastercard will provide risk-scoring solutions that may be helpful for our customers. The solutions will be particularly useful for those customers that intend to apply the TRA exemption.

Mastercard will also offer packaged solutions that will significantly ease the burden of compliance and reduce the impact on in-house IT development. These solutions group together a number of existing Mastercard hosted products.

Rules changes to facilitate use of exemptions

Mastercard believes that the benefits of the exemptions from SCA are significant as they make one-click payments possible. Mastercard is changing its Rules to facilitate the application of the exemptions and a shift in liability. Mastercard encourages its customers to apply all the exemptions, where permitted.

The white-listing exemption is important to enable one-click payments for card-on-file (CoF) payments and allow for recurring payments for variable amounts (e.g., bill and utilities payments, and subscriptions to digital services). The Issuer’s Masterpass wallet and the Issuer’s ACS provider are best placed to support white-listing of merchants on the issuer’s behalf with minimum impact on Acquirers and Issuers. Mastercard recommends that Issuers ensure their Masterpass wallet and ACS providers support white-listing of merchants. Issuers and Acquirers are encouraged to explain to cardholders and merchants the benefits of white-listing.

The TRA exemption is allowed under certain fraud levels and transaction amounts. This exemption is based on the concept of Risk Based Authentication (RBA). RBA is a process where the Issuer (or the Acquirer) evaluates the fraud risk of a transaction and SCA is not applied if the risk is low.

Before the RTS apply in 2019, Mastercard recommends the use of RBA. Once the RTS apply, Issuers and Acquirers are encouraged to apply the TRA exemption, provided their fraud rate is below the reference fraud rate and the transaction amount is below the Exemption Threshold Value, as defined in the RTS.

In order for all customers to benefit from the TRA exemption, Mastercard will introduce rules on how best Acquirers should apply this exemption. Liability will be shifted to Acquirers when they apply the TRA exemption.

Finalization of Mastercard's authentication infrastructure

Mastercard is completing the development of the infrastructure to support the new authentication requirements. Support for customers is already planned 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.

Publication of Safety & Security Announcements

Mastercard has decided to change its Rules to help our customer provide a better authentication experience and facilitate the use of exemptions in Europe. These changes are published in our Safety & Security Announcements. Mastercard will publish further Announcements in its aim to help customers comply with the regulation.

3. The new regulatory requirements for SCA

The following is a list of questions regarding the new regulatory requirements. The answers are provided to the best of our knowledge and do not constitute legal advice. Customers are encouraged to speak with their legal counsel for guidance.

What is SCA?

The RTS define SCA as authentication through at least two out of the following three factors:

- Something only the user knows (e.g., passcode or PIN);
- Something only the user possesses (e.g., mobile phone or token);

- Something the user is (e.g., fingerprint, facial, iris or eye vein).

The RTS require that the selected factors must be mutually independent in that the breach of one does not compromise the reliability of the other (Article 9 RTS).

The use of a single device for authentication and shopping is expressly permitted. This means, for example, that a smartphone can be used at the same time for transacting and for authenticating the cardholder. The risk connected to the use of multi-purpose devices (e.g. smartphones and tablets) must be mitigated through the use of separated secure execution environments. Mechanisms to ensure that the software or device have not been altered by the payee or by a third party must be in place, as well as mechanisms to mitigate the consequences of such alteration.

What is dynamic linking?

For remote transactions, each SCA must be linked to a specific amount and payee (dynamic linking). This requirement, effectively binding authentication to the merchant and the amount, aims at ensuring that a valid authentication code is only used once and for the specific transaction for which the authentication is requested (Article 5 RTS). This aims to reduce “man in the middle” attacks where an authentication code is used for a different (fraudulent) transaction.

The dynamic linking requirements can be summarized as follows:

- The cardholder must be made aware of the merchant details and amount when asked by the Issuer to authenticate herself / himself.
- The authentication code generated by the Issuer can only be used once and must be linked to the specific merchant and amount displayed to the cardholder.
- The authentication code must successfully authenticate only the transaction linked to those specific merchant and amount.
- The resulting cryptographic token must be passed by the Acquirer in the authorisation request and must be unique for that specific transaction.
- The Issuer must validate the cryptographic token passed in authorisation and ensure that there is a match in merchant and amount between the token and authorisation.
- If there is no match, the Issuer should decline the transaction.

When will SCA apply?

SCA is required when the payer initiates an electronic payment transaction (Article 97 PSD2). Exemptions may apply (Article 98 PSD2). The regulation also mandates SCA for any action through a remote channel that may imply a risk of fraud (e.g., initial registration of a card in a wallet or in a Card on File solution).

Conversely, SCA is not required for Mail & Telephone order (MoTo), anonymous prepaid and direct debit transactions.

Which transactions are exempted from SCA?

While SCA is the rule for electronic transactions, the use of alternative authentication measures is permitted if an exemption applies. The use of exemptions remains optional and is not mandatory. The following table contains a list of the exemptions that are discussed in this document:

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

White-lists of trusted beneficiaries. What is white listing?

Cards benefit from the white-listing exemption (Article 13 RTS). The payer can request her/his Issuer to white-list a payee (merchant) so that SCA is not required on subsequent transactions to that payee. Issuer must apply SCA when the cardholder adds, deletes or amends white-listed merchants.

Issuers can develop their apps and banking website to allow white-listing for cards. ACS providers can play an important role by requesting the cardholder to white-list a trusted merchant while shopping. For example, the cardholder could tick a box to white-list the merchant when authenticating the transaction. One single SCA may be sufficient for authenticating the transaction and simultaneously white-listing the merchant.

White-listing is important to enable one-click payments for cardholders, to allow for CoF payments and for recurring payments for variable amounts, which would otherwise require SCA. For these transactions, one SCA for the initial transaction and simultaneous white-listing of the merchant may be sufficient. In this way, the customer experience will be very similar to that of a direct debit (for which only the initial e-mandate requires SCA).

What is the TRA exemption?

This exemption especially allows Issuers and Acquirers to balance the need for SCA against friction at checkout. It applies to remote payments. Stringent conditions are provided for the application of this exemption (Article 18 RTS).

Merchants cannot apply this exemption directly but can rely on their Acquirer applying the exemption. In this case, the Acquirer will be liable for the transaction.

To take advantage of the TRA exemption, the customer that is applying the exemption must enjoy a gross fraud level up to 13bps in a quarter. The actual fraud level determines the maximum exempted transaction value (ETV), as per the table below:

ETV	**Reference fraud rate (bps)**
EUR 500	*1*
EUR 250	*6*
EUR 100	*13*

The formula to calculate the reference fraud rate for the application of the TRA exemption is total value of unauthorized and fraudulent remote card transactions divided by total value of all remote card transactions.

The following should be noted:

- All remote card transactions should be considered for the calculation regardless of whether (1) they are subject to SCA or (2) they fall under an exemption.
- Face-to-face transactions are excluded from the calculation of the fraud rates.
- The total value of unauthorised/fraudulent remote transactions should be gross, i.e. regardless of whether the funds have been recovered or not. Thus, chargebacks should not be included.
- All remote card transactions regardless of brand (e.g., Mastercard, Visa, Amex) or product (debit, prepaid or credit) should be considered for the calculation.
- Non-EEA volumes and frauds are excluded from the calculation of the reference fraud rates. Also transactions in the EEA with cards issued outside the EEA are excluded.
- Customers should calculate the fraud rate across all values and then choose the Exempted Threshold Value (ETV) band that is allowed.
- Transactions above the ETV for which a customer qualifies, and any transaction over €500, must be undertaken with SCA (unless another exemption applies).

The customer that is applying the exemption will have to maintain or improve on its fraud levels. If the customer exceeds 13bps of fraud in two consecutive quarters, the customer must immediately cease to use the exemption (Article 20 RTS). Evidence will need to be provided that rates have been maintained below that rate for an entire quarter before the customer will be eligible to use this exemption again. The customer must have its fraud data audited and, upon request, make the audit available to its national competent authority.

How are recurring transactions impacted?

An exemption applies for recurring transactions with the same amount and with the same payee (Article 14 RTS). This means that a series of recurring transactions to the same merchant is exempted provided the amount is unchanged (e.g., a monthly bill payment for the same amount). The first transaction of the series must always be undertaken with SCA. Mastercard will clarify in its Rules how to flag these transactions.

Conversely, recurring transactions for a variable amount are not expressly exempted. Issuers are strongly encouraged to offer their consumers the option to white-list trusted merchants to allow for recurring payments for a variable amount (e.g. bill payments, subscriptions for digital services) to occur at these merchants without SCA after the first authenticated transaction. To this end, the cardholder can use one single SCA to authenticate the first transaction and white-list the merchant.

Card on File merchants. Are there exemptions available?

Card on File (CoF) merchants provide a better consumer experience at check-out. The merchant offers the shopper to store her/his card details, such as PAN and addresses, so that this information does not have to be keyed in on every occasion the cardholder initiates a payment.

The RTS do not contain a specific exemption for CoF transactions. SCA is required on every transaction that the cardholder initiates with the stored details, except if an exemption applies. White-listing is particular relevant to allow for one-click payments with CoF, especially because the cardholder can use one single SCA to authenticate the transaction and simultaneously white-list the merchant.

How does the exemption for low-value remote payments work?

This exemption applies to remote transactions up to €30, with a maximum of €100 cumulative spend or 5 consecutive transactions since SCA was last applied (Article 16 RTS). The Issuer is allowed to choose alternatively between the €100 cumulative spend or 5 consecutive transactions to apply the exemption. This means that SCA must apply only to the 6th (or subsequent) transaction exceeding the cumulative spend of €100.

What is the impact on contactless payments?

Contactless payments provide convenience to cardholders and reduce cash usage. Exemptions are provided for low-value contactless transactions (LVTs) up to €50 with a maximum of €150 cumulative spend or 5 consecutive transactions (Article 11 RTS). This means that if at least €150 (cumulative) worth of contactless transactions are made at a point of sale, and 5 transactions below the contactless no-CVM limit are made, then the terminal would need to ask for SCA to be applied for the next transaction (even if that transaction would qualify as a no-CVM transaction).

The regulation does not clarify how the exemption for contactless LVTs must be managed when a PAN is digitized in one or more devices. In this case, it is not clear whether the exemption should be managed at the account level (taking into account all contactless transactions for a specific account across all devices) or at the device level (taking into account only the contactless transactions for each individual device). Mastercard is advocating with national competent authorities that the exemption for contactless LVTs be applied at device level, as this would require a less complex technical implementation. The application of the exemption at device level would lead to reduced fraud levels and ensure safety and security of payments.

Which exemption will commercial cards benefit from?

Business-to-business payments over dedicated payment processes and protocols are exempted. This exemption will apply to "payment processes or protocols that are only made 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 (Article 17 RTS).

Although this leaves the decision with the competent authority of each Member State, we believe that the following examples of commercial transactions should be exempt:

Lodged cards: A commercial card that is lodged with a company-approved third party, such as a travel company that books travel and hotels on behalf of the company by secure dedicated payment process and protocol, is exempted. Use cases include both traditional company travel procurement (via a company-approved travel agency) and broader business-to-business procurement, where commercial cards are lodged securely directly with approved company suppliers.

Use of a commercial card by an employee him/herself at a public website for the purchase of equivalent goods or services (such as travel or accommodation) is instead not exempted as this transaction does not use a secure dedicated payment process and protocol.

Virtual Card Numbers: Virtual card numbers (VCNs) used over dedicated payment processes and protocols ensure a very high level of security. The generation of VCNs is protected with SCA and the virtual PAN itself can also be uniquely linked to the merchant or other parameters that further control its use (e.g. amount, time). SCA at the time of use is therefore not required.

What is the exemption applicable to unattended terminals for transit and parking?

SCA is not required for (contact and contactless) transactions for paying a transport fare or a parking fee at unattended payment terminals, regardless of amount (Article 12 RTS). Thus, this is not a general exemption for all unattended terminals.

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 authorization as they indicate the risk of the transaction. Transactions with a score indicating high risk should be declined in authorization, even when fully authenticated. An enhanced form of transaction monitoring is mandated for the application of the TRA exemption.

Is card data a valid authentication factor?

Mastercard believes that card data (PAN, cardholder's name, expiration date, CVC) is a valid authentication factor. Certain national competent authorities have already confirmed that card data is a knowledge factor (others take a different approach).

Mastercard believes that tokenized card data is also a valid authentication factor. When associated univocally with a device, the token cannot be used from another device. This makes the token an ownership factor.

Is delegated authentication to a smartphone allowed?

There are a number of devices (e.g. smartphones) that include a Consumer Device Cardholder Verification Method (CDCVM) to access the device. This is a great opportunity for these devices to be used by consumers to authenticate themselves for a payment, especially for mobile NFC payments, as most of them occur via x-Pay wallets (e.g., Apple Pay). Mastercard believes that Issuers are allowed to rely on the CDCVM to authenticate their cardholders, provided Issuers always securely associate the device (and its CDCVM) by applying SCA for the initial enrolment of a card in the wallet (or x-Pay wallet). Mastercard is considering setting network security standards of a shared CVM, which examines both the types of CVM in use (biometrics, swipe patter, PIN etc.) and the technical requirements for the device to be securely used for authentication.

Is delegated authentication to a merchant allowed?

Mastercard is considering whether Issuers are allowed to rely on the security credentials issued by the merchant to authenticate cardholders, provided the security credentials are compliant with the SCA requirements under the RTS (for example, they allow for secure biometric authentication). This would require SCA by the Issuer for the association with the cardholder of the credentials issued by the merchant and an express delegation by the Issuer. In addition, it would only be allowed for low-risk merchants and provided the card is digitized and tokenized in the CoF solution of the merchant. This could be managed through a Mastercard program (e.g., 'Express', which currently regulates Issuers' participation to the x-Pay wallets through MDES). Merchants could bear liability for these transactions, if permitted by national competent authorities.

Is persistent authentication for wearable devices allowed?

Persistent authentication means that authentication occurs continuously throughout the cardholder's operation of a wearable device, typically through continual contact with human body or biometric monitoring (for example, the monitoring of a heartbeat). The RTS are technologically neutral and do not expressly regulate wearable devices. We believe that they are compliant with the RTS provided that they continuously apply SCA (e.g. through a token in the wearable device associated with SCA by the Issuer or sufficiently secure unlock mechanism). The dynamic linking requirement does not apply to face-to-face transactions with wearable devices.

How will the exemptions' Euro limits apply for transactions in other currencies?

The RTS set out transaction amount limits for the application of the TRA exemption and the exemptions for low-value remote payments and contactless transactions. The RTS express these limits only in Euro. For transactions in non-euro currencies, national competent authorities or national acts may set a national currency equivalent. Where this does not occur, card schemes and customers may set a (rounded) currency equivalent.

4. What are the key decisions I need to make as an Issuer?

Biometric Authentication

Mastercard believes that biometrics will play an important role in authentication. Cardholders find biometrics increasingly familiar thanks to smartphone penetration. Smartphones increasingly use some form of biometrics, fingerprint and facial recognition to unlock the device. Device manufacturers have been training consumers to accept this as normal practice.

Some customers have already taken steps to deploy this technology. When biometric authentication is used, Issuers report that abandonment rates typically drop by 70% compared to other methods (e.g., an OTP sent via SMS). This reflects the much improved user experience.

In order to guarantee security and reduce friction at checkout, Issuers should offer biometric authentication. To this end, Issuers will have to:

- Ensure that biometric authentication methods meet industry standards, e.g. NIST SP800-63-3 (see https://pages.nist.gov/800-63-3/).
- Ensure that cardholders are authenticated via a single mobile application to avoid separate authentication processes for different transaction types. A single authentication experience is key for cardholders. The Issuer's mobile banking application should embed payment and authentication functionalities and provide the same biometric authentication user experience for card payments and mobile banking.
- Offer at least 2 biometric modalities, including fingerprint and another method (such as using facial or voice recognition) to allow as many cardholders as possible to benefit from biometric authentication. It is also recommended to add new biometric modalities when they become available on mobile devices and their security is tested (for example, iris scan, behavioural biometrics).
- Increase the penetration of their mobile banking applications, as this will be crucial for their cardholders to use biometrics. Advertisement campaigns explaining the benefits of security and convenience of these apps will need to be deployed.
- Offer an alternative authentication method for cardholders without a smartphone. For example, offering an OTP sent via SMS could be a fall-back authentication method.

Issuers should avoid adopting solutions such as card readers or other hardware token generators, which are inconvenient for mobile users, and passwords, which are easy to forget.

Mastercard is mandating that Issuers offer their customers biometric authentication for Mastercard Identity Check/SecureCode and Masterpass transactions, including NFC mobile transactions.

White-listing

Mastercard strongly recommends Issuers to support this exemption, given the improved cardholder experience and potential for increased volumes. The white-listing exemption will be vital to enable one-click payments for CoF payments and for recurring payments for variable amounts.

To enable technically this exemption for cards, Issuers can upgrade the banking white-list solutions that are currently used for credit transfers to also be used for cards. ACS providers can also enable white-listing during shopping.

The consumer experience for white-listing is key. It should be at least as good as the one for a direct debit e-mandate. Otherwise, Issuers risk being disintermediated by direct debit (as direct debit requires SCA only for the e-mandate).

Issuers should limit the white-listing to low-risk merchants (e.g., based on MCC or a list of low-risk merchants). As per any other transaction, Issuers must closely monitor transactions at white-listed merchants. Issuers should apply SCA on transactions at white-listed merchants when the transaction is not low-risk (e.g., a new shipment address is used for the transaction).

Transaction Risk Analysis (TRA) Exemption

The use of the TRA exemption has considerable benefits. Friction at checkout can be eliminated and one-click payments are made possible. This will not increase the risk of fraud beyond acceptable parameters. Customers are therefore strongly recommended to apply this exemption.

Mastercard is deploying Mastercard Decision Intelligence to help issuers drive their fraud level down and apply the TRA exemption. MasterCard Decision Intelligence is an independent risk management layer to help issuers augment their existing fraud defenses and protect the integrity of their brand. This solution provides an additional layer of powerful fraud insights via a score, which is added to the authorization message. The score can then be fed into an issuer’s local rules engine. Alternatively, decline rules can be deployed at the Mastercard network level via the self-service Security Utilities in the Fraud Center on Mastercard Connect. Using the self-service Security Utilities in the Fraud Center on Mastercard Connect, Issuers can write decline rules to alert or decline transactions, which are deployed prior to the transaction reaching the processor.

Other exemptions

Mastercard recommends that Issuers use the exemption for low-value remote payments and all other available exemptions.

Card on file

Issuers must always apply SCA for enrolment of their cards in CoF solutions. Mastercard strongly recommend that Issuers enable white-listing for trusted merchants so that subsequent CoF transactions will not require SCA.

CVM Delegation

Issuers must always apply SCA for enrolment of their cards in wallet solutions, including on mobile devices. Issuers should verify and audit the security measured related to the devices and wallet solutions on which their cards are used.

5. What are the key decisions that I should make as an Acquirer?

White-listing

Given the importance of this exemption to ensure a competitive position of cards vis-à-vis other payments means, trusted merchants should suggest to their customers to white-list them. Acquirers should encourage their merchants to do so.

Risk-Scoring

In order to properly risk-score a transaction, it is very important to combine the merchant and Acquirer's knowledge of a cardholder with that of the Issuer. The information flow from the merchant to the Issuer is very useful to this end. Acquirers need to review all existing merchant relationships that undertake remote electronic payments and ensure that they deploy EMVCo 3DS 2 (or alternative technological SCA solutions).

TRA Exemption

Pursuant to the RTS, merchants are prohibited from directly applying the TRA exemption. However, Acquirers may apply this exemption and are strongly encouraged to do so. Acquirers will bear liability when applying the TRA exemption.

Card on file

CoF associated with white-listing provides a convenient solution allowing for one-click payments. Acquirers should encourage CoF solutions with white-listing at their merchants. The cardholder must apply SCA through the Issuer for the white-listing.

6. Conclusions

Security is important to gain consumer trust. A seamless customer experience is key to reduce friction at checkout. Biometrics will drive conversion and approval rates up.

Issuers and Acquirers are encouraged to apply the exemptions to reduce friction even further. This will ensure the competitiveness of our products.

Mastercard will continue to work with its customers and offer authentication and risk-based fraud assessment tools to help them comply with the regulation.

Mastercard would be pleased to discuss these solutions with our customers. We encourage our customers to discuss their potential interest with their Mastercard account team.

* * *