Digital payments require Strong Customer Authentication as of September 2019 – will you be ready?

Understanding the changes and opportunities of PSD2

Reduce fraud and false declines of card-not-present (CNP) transactions – with an enhanced check-out experience for cardholders

The EU second Payment Services Directive (PSD2) aims to reduce fraud and introduces higher security standards for online payments.

Strong Customer Authentication (SCA) – also known as 2-factor authentication - must be used for all remote electronic transactions, from the 14th September 2019 - unless an exemption applies.

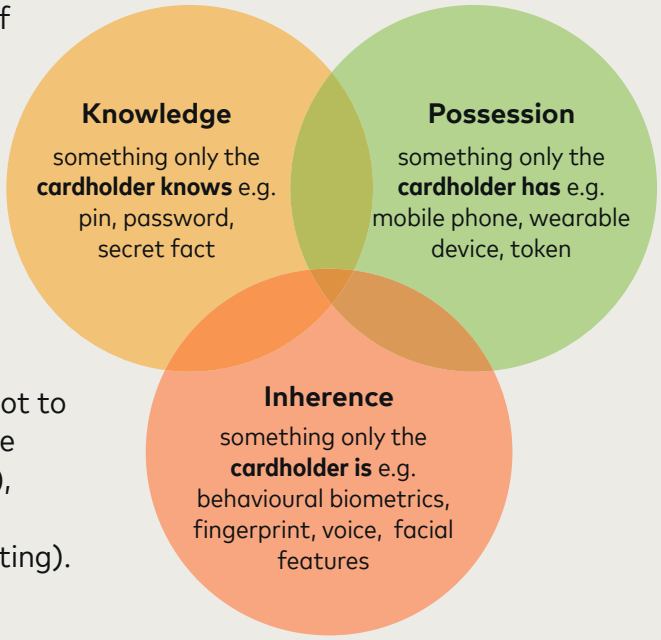
Merchants must send authentication requests using the new EMV 3-D Secure (EMV 3DS) protocol – otherwise issuers might decline the transaction to avoid non-compliance.

Strong Customer Authentication (SCA) is a mandatory pillar of PSD2, ensuring a high level of payments security

SCA means authentication based on the use of two or more independent elements, which are categorized as 'knowledge', 'possession', or 'inherence'.

It applies to transactions where issuer and acquirer are both based in EEA countries.

PSD2's Regulatory Technical Standards (RTS) provide for a number of exemptions allowing not to insist on SCA for transactions, e.g for low-value payments (equal/below €30, conditions apply), repetitive transactions (same amount) and transactions to trusted beneficiaries (white listing).



Why act now?

Not using SCA could result in increased levels of declined transactions which can create customer dissatisfaction and impact your sales.

If executed well, SCA increases online payments security and convenience, plus lead to greater customer loyalty.

To comply with PSD2 and Mastercard rules online merchants must support EMV 3DS authentication requests as of April-December 2019 (depending on country).

With EMV 3DS and Mastercard® Identity Check™, e-commerce merchants will be able to achieve the same performance levels as physical store merchants*

50%
up to 50% reduced fraud rates

10%
on average 10 percentage points higher approval rates

50%
around 50% lower abandonment rates

* Physical store merchants using Chip & PIN, as measured on the Mastercard network / transaction data 2017

EMV 3DS is projected to become one of the strongest solutions in the fight against card-not-present (CNP) fraud - without sacrificing the shopping experience.

EMV 3DS is the new 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.

Mastercard ID Check helps improve digital payments security and increase approvals – while offering a frictionless payment experience

Mastercard® Identity Check™ leverages the updated EMV 3-D Secure protocol to help reduce fraud, false declines and unnecessary friction - while meeting Strong Customer Authentication (SCA) requirements under PSD2 regulation. It enables merchants and issuers to take advantage of the new capabilities to help drive simple and secure payments.

Why mastercard ID Check

1. Supports all digital devices, including mobile or in-app payments
2. Enhanced decisioning via increased data flow
3. Enables state-of-the-art authentication methods, such as biometrics, for higher approval rates, also supporting dynamic passwords, security questions, or proprietary options
4. Replaces SecureCode®, delivering a better online payment experience for consumers by reducing cardholder verification needs
5. Supports new use cases like credentials-on-file (CoF), wallets, tokenisation

Speak to your Acquirer and Gateway today!

Your Acquirer and Gateway will help ensure that your payment process meets PSD2 requirements so that you continue to seamlessly accept payments on 14th September 2019.