Safer payments made simple

A short introduction to Europe's new requirements for **Strong Customer Authentication**

Worldline

In brief

Even if most European countries have granted a grace period to the application of Strong Customer Authentication (SCA), giving time after September 14, 2019 for its application, Strong Customer Authentication remains mandatory by law for merchants across Europe.

In accordance with the EU's second payment services directive (PSD2[1]), this means that banks will frequently require more information from a merchant's customer than just their name, card number and card security code.

Merchants and their Payment Service Providers (PSPs) will have to be able to authenticate a customer's identity for card payments using the 3-D Secure (3DS) protocol, which supports a variety of technologies ranging from One Time Passwords to fingerprints and facial recognition. If SCA and 3DS are not enabled by the merchant's PSP, a transaction could be declined by a customer's bank.

Smart, simple and seamless

Many merchants are understandably concerned about the possible impact of these requirements on their e-commerce volumes. Yet as well as countering rising levels of online fraud, the new rules will make it easier for genuine customers to make legitimate purchases online. The EU technical standards[2] that implement PSD2 will provide online shoppers with a safer and more user-friendly experience, especially when using their smartphones.

Many low-value transactions and recurring payments will be exempt. The additional verifications will not be required for most online transactions under €30. Intelligent, risk-based authentication will lead to fewer disruptions of payment. In the event that cardholders are requested to prove their identity, they will no longer be redirected away from the merchant's website to enter their details on a new payment window. Customers will be able to authenticate their identity as a seamless part of the checkout process, reducing the risk of drop-offs.

This is happening, soon

Most European countries have granted a transition period following September 14, giving all players in the market more time to migrate to the new environment. Whereas the duration of this transition period is not known, it is sure that is only temporary. Merchants need to make sure now that their PSPs are compliant with the authentication requirements. Merchants should also review their online payment models and redesign their checkout processes, incorporating the steps needed to support 3DS, enable strong authentication and improve customer experience.

The new rules may seem challenging, but if implemented correctly and with the necessary expertise they will make online shopping safer and more user-friendly, with the potential to increase conversion rates and lift e-commerce volumes across Europe.

---

[1] Directive 2015/2366/EU (PSD2)

[2] Regulation (EU) 2018/389 – Regulatory Technical Standards on strong customer authentication and secure communication

A safer place to shop

Many online merchants in Europe are already familiar with the form of customer authentication known as 3-D Secure 1.0. Developed by the major credit card schemes, this procedure involves redirecting cardholders to an external web page or pop-up window. In order to verify their identity, customers must enter a code or a password, which can all too easily be forgotten.

This process can result in high levels of drop-offs and is not well suited to transactions on mobile phones. As a result, there is some reticence among retailers across Europe, with many merchants having chosen not to implement the protocol at all.

As the SCA requirements of PSD2 come into force, ignoring 3DS is no longer an option for merchants. Issuing banks may decline online payments that have not been authenticated using 3DS. Fortunately for merchants concerned by this prospect, help is at hand in the form of 3DS 2.0: a modern specification which is fully compliant with the new rules and reflects current and future market requirements to provide a more secure and smoother experience for users.

Seamless security

3DS 2.0 has been specifically designed by the card schemes not only to improve the security of e-commerce but also to enhance the customer experience, especially on smartphones and when making in-app purchases and using digital wallets. It results in a cardholder authentication process that is both more secure and more straightforward.

On the security side, in compliance with the SCA requirements, 3DS 2.0 will rely on two-factor authentication. A static password will no longer suffice. Customers will have to authenticate their identity by using elements from two of the following three:

Knowledge

Something the customer knows (e.g. password, PIN, secret question)

Possession

Something the customer has (e.g. mobile phone, wearable device, bank-provided security token)

Inherence

Something unique to the customer (e.g. fingerprint, voice, iris or face recognition)

Currently, one technology extensively used to enable two-factor authentication is the temporary One-Time Password (OTP) sent to a device owned by the customer, such as a mobile phone, security token or a wearable such as a smart watch. In the future, secure authentication based on the biometric elements of Inherence are likely to become widespread. Many banks in Europe are now accelerating their development of these intuitive, user-friendly technologies, which are supported by 3DS 2.0 (but not by 3DS 1.0). The sophisticated 3DS 2.0 also represents a significant improvement in the user experience when compared with the previous version. When two-factor authentication is required, 3DS 2.0 integrates the authentication process into the checkout stage of a merchant's website or mobile app, removing the need for a redirect.

While 3DS 1.0 as it stands is compliant with the new SCA requirements, it is expected to be phased out around the end of 2020. All issuers and merchants will then have to use 3DS 2.0. Many payment players are now beginning to migrate to the latest version, which minimizes friction and reduces the risks of cardholders abandoning their transactions.

Frictionless flow

An important principle of the new SCA requirements is that cardholders should be required to prove their identity only during those online transactions in which the risk of fraud is considered to be higher.

Transactions such as mail orders, telephone orders, and transactions outside the European Economic Area are not included in the scope of the new rules. Merchant-initiated transactions such as payments taken with the cardholder's consent and initiated by the merchant, like utility bill payments, also fall out of the scope of SCA. Furthermore, many transactions will be exempted, using analyses of data shared by the merchant with the issuer.

Low-risk transactions may be eligible for a wide range of exemptions from two-factor authentication. These include:
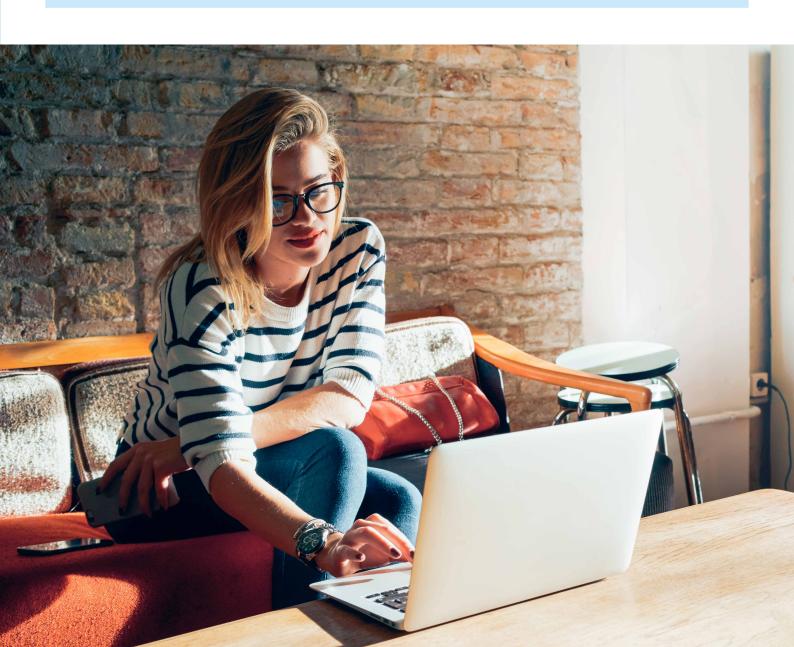
- **Low-value transactions.** Remote electronic transactions below €30 will be exempt, unless their total value reaches €100 or a total of five transactions are made.

- **Transaction Risk Analysis.** An exemption can be granted based on the average fraud rates of the acquirer and issuer. The lower the fraud rate, the larger the transaction that can be processed without an SCA challenge.

- **White-listed merchants and Trusted Beneficiaries.** Transactions with a merchant can qualify for an exemption after a consumer has added that merchant to a white list as a trusted beneficiary.

- **Recurring transactions** such as subscriptions.

- **Corporate payments.**

For all these exemptions, merchants will be able to enjoy so-called "frictionless flow". Online payments covered by these transactions will be authorized automatically, without the need to request customers to confirm their identity. 3DS will only be triggered when these exemptions do not apply.

Merchants cannot apply for these exemptions by themselves; only acquirers can request the implementation of the SCA exemptions. The issuing bank then has the ultimate responsibility for granting any exemption that is requested. Issuers may still demand Strong Customer Authentication, even when the merchant's acquirer requests the exemption for Transaction Risk Analysis.

Of particular value to merchants will be the exemption for Transaction Risk Analysis, which will reduce the potential for SCA challenges and for drop-offs at the checkout. In addition, because banks with lower fraud rates will be able to provide merchants with higher levels of frictionless flow, there will be an added incentive for acquirers to improve their online security levels.

What merchants need to do

Following a recommendation of the European Bank Authority done in July 2019 that is to provide a grace period for the application of the RTS, most of the European National Competent Authorities have granted a grace period to the PSPs they regulate. The following countries already announced this PSD2 enforcement delay through their local authorities: Austria, Belgium, Denmark, Germany, Ireland, Italy, Luxemburg, Malta, Netherlands, Norway, Sweden, Slovenia, UK. **Therefore, transaction flow processed before September 14th remains compliant after Sept 14th.**

By the way, because the conditions of application and the duration of this grace period have not been communicated yet by the local regulators and because the issuing banks located in EEA countries without transition period could require SCA to approve the transaction, retailers need to start preparing for Strong Customer Authentication and 3DS now.

As a first step, merchants should contact their PSP to confirm that they support at least 3DS 1.0 for SCA and will be compliant with the new regime. If a PSP cannot support SCA, an issuer bank may decline to authorize a merchant's non authenticated transactions.

Although 3DS 1.0 is compliant with SCA for now, a PSP should also have in place a roadmap for migrating merchants to 3DS 2.0 when the improved protocol is supported by banks. PSPs must explain how merchants will be affected by the new requirements and what they are doing to ensure full compliance with SCA.

Merchants will also need to discuss the exemption rules with their PSPs and acquirers and agree which exemptions to request in order to achieve frictionless flow. The management of exemptions will be essential to reshaping the online payment experience and increasing the confidence of cardholders.

If an acquirer does not request the exemptions on behalf of a merchant, issuers may demand strong authentication for all online transactions covered by the rules, potentially reducing the merchant's conversion rates.

By working closely with their PSPs and acquirers, merchants will be able to minimize the number of authentication requests from issuers and ensure high levels of frictionless flow. As various markets and banks may interpret the rules differently during the transition period, it is important at this time for merchants to develop strong partnerships with their PSPs and acquirers.

A fresh look at payments

For their part, merchants need to review their payment processes and flows to take advantage of these changes and improve the experience of their customers. They may have to implement new APIs to benefit from 3DS 2.0. If a bank requires strong authentication for a transaction, a merchant must be ready to support SCA as seamlessly as possible, minimizing any inconvenience to online shoppers.

Merchants may also want to take the opportunity to positively engage with their own end-users about any changes they will see when making online payments in future.

All players in the payments ecosystem, from banks to PSPs to merchants, will need to ensure that the e-commerce marketplace adapts to the new rules with the minimum of disruption.

The long-term result of SCA and 3DS 2.0 will be lower rates of fraud in e-commerce, higher cardholder confidence and increased convenience. With a simpler and more secure payment process, merchants may expect to see higher online conversion rates when the new rules are implemented.

Worldline: ready to deliver

Worldline was one of the first payment providers in Europe to process 3DS 2.0 transactions in a live environment. In Q4 2018, we launched a project with banks, card schemes and a selected group of merchants, leading to a pilot phase which since May 2019 has been authenticating real-world transactions with 3DS 2.0.

Thanks to our payment acceptance solution, which is dedicated to securing and managing e-commerce payments, we are the clear-cut European partner of choice for merchants looking to maximize frictionless flow, manage exemptions and optimize online user experience.

Worldline experts have been sharing our expertise and practical experience in this area over the course of the past year in a series of workshops with merchants, PSPs and banks to explain how payment platforms can effectively apply 3DS 2.0.

We are already working with a growing number of merchants of all sizes to deliver compliance with the new regime. Our experts are ready to help all merchants successfully embrace these challenges and reap the benefits of online payment processes that will be safer, smarter and easier to use.

About Worldline

Worldline [Euronext: WLN] is the European leader in the payment and transactional services industry. With innovation at the core of its DNA, Worldline's core offerings include pan-European and domestic Commercial Acquiring for physical or online businesses, secured payment transaction processing for banks and financial institutions, as well as transactional services in e-Ticketing and for local and central public agencies. Thanks to a presence in 30+ countries, Worldline is the payment partner of choice for merchants, banks, public transport operators, government agencies and industrial companies, delivering cutting-edge digital services. Worldline's activities are organized around three axes: Merchant Services, Financial Services including equensWorldline and Mobility & e-Transactional Services. Worldline employs circa 11,000 people worldwide, with estimated pro forma revenue of circa 2.3 billion euros on a yearly basis. worldline.com

For further information
infoWL@worldline.com