SECURITY

Strong customer authentication

Frequently asked questions

Strong customer authentication: frequently asked questions

Strong customer authentication and its impact on the check-out process has been top of mind for those who trade online for the last couple of years.

With more clarity on the requirements and the implementation deadline set for the end of 2020, we answer the most frequently asked questions from customers and partners.

What is strong customer authentication?

Strong customer authentication is part of the revised Payment Services Directive (or PSD2), a package of measures introduced by European regulators, to help make online banking and payments more secure. From 31 December 2020 in the EU (and 14 March 2021 in the UK), every electronic transaction will require strong customer authentication, except in a very few cases. The changes will impact everyone: consumers, those who accept electronic payments, and those who provide payment and banking services in Europe and the UK.

How is strong customer authentication achieved?

Sometimes also known as multi-factor authentication, strong customer authentication means that payment providers must ask for, and customers provide, two or more of the following 'factors'. This will better determine whether someone is really who they claim to be.

Description		Example
Something the payer knows	Knowledge	Password, PIN, memorable information Pre-
Something the payer has	Possession	registered mobile phone, card reader, token
Something the payer is	Inherence	Fingerprint, iris scan, facial recognition

We answer the most frequently asked questions from customers and partners.

pxp

Who has enforced it and why?

Changing shopping habits, lifestyles and technology are putting pressure on traditional, static, knowledge-based authentication methods, such as passwords. Customers are shopping more and more online. 71% of internet users in the EU shopped online in 2019. And 35% of e-buyers made purchases from sellers in other EU countries, compared with 2% in 2014, according to eurostat. As fraudulent activity tends to follow sales volumes, e-commerce fraud is also growing. This may inhibit consumers' willingness to spend online. Regulators hope that the new requirements will protect consumers, drive the digital agenda, competition and security across Europe.

The idea of authenticating customers for online purchases is not new. 3D Secure, the protocol that sits behind Verified by Visa, Mastercard SecureCode and other authentication solutions, has existed for around 20 years. International card schemes have long encouraged take- up of 3D Secure for online card payments. They offered liability shifts for card issuers and acquirers to incentivise adoption. However, there were drawbacks. Acquirers and their merchants were not always mandated to use 3D Secure. Cardholders were not enrolled. Passwords were static and the protocol not optimised for all devices. As such, the customer experience wasn't always great and basket abandonment high.

The first version of 3D Secure (3DS 1.0) complies with EU strong customer authentication requirements. However, the new version (3DS 2.0) addresses many of the above issues. It's optimised for any device type as well as for in-app payment. Merchants can pass more information to issuers for better risk scoring. And various current and future authentication methods are supported. All of which improves the online check-out experience.

Whatever value-added services you're looking for, PXP can provide them.

[1]E-commerce statistics for individuals, eurostat, January 2020, https://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#E-shopping:_biggest_increase_among_young_internet_users

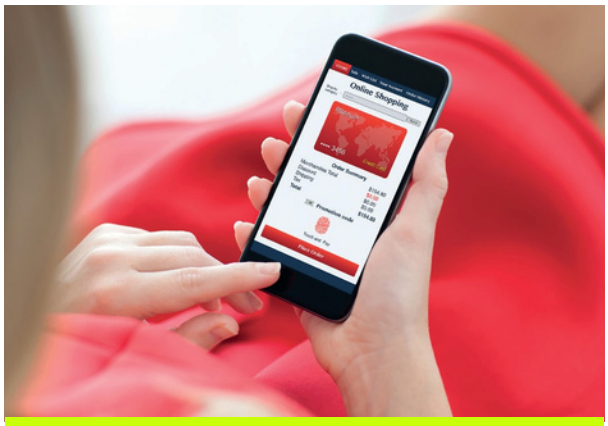
pxp

Why is it so important?

The new strong customer authentication requirements are a significant change to the current e-commerce model for card payments. Previously the decision to adopt 3D Secure was largely optional and managed contractually between merchants and their acquirers. However, from 2021 strong customer authentication will be compulsory for every e-commerce transaction, unless an exemption applies. Secondly, the responsibility for authenticating customers will sit with service providers (issuers and acquirers in the case of card payments), not merchants. The authentication model is moving from opt-in to mandatory.

How does it effect cardholders and merchants?

Cardholders may be asked for additional information when they make a card payment online. If the nature of the transaction is deemed as low risk by the card's issuer, such as you always order a takeaway via the same company, on the same device, using the same card at regular intervals) then there will be no request for additional information – this is referred to as "frictionless flow".



In cases where the transaction is deemed as high risk by the card issuer, such as buying a new TV at 3am on a device you've never used before, then the card holder will be asked for additional information by the card issuer to verify they are who they say they are, using 2 of the 3 factors – this is referred as "challenge flow".

Regulators hope that the new requirements will protect consumers, drive the digital agenda, competition and security across Europe.

pxp

What are the exemptions to strong customer authentication requirements?

The following scenarios are exempt or out of scope from EU strong customer authentication (SCA) requirements:

1. Anonymous transactions
   For example prepaid gift cards not issued to an identifiable person.

2. Contactless payments
   Face-to-face transactions at contactless readers up to €50, or equivalent in the processing currency, with a cumulative limit of €150 or five consecutive transactions.

3. Low-value ecommerce payments
   Transactions up to €30, or equivalent in the processing currency, with a cumulative limit of €100 or five consecutive transactions.

4. Mail order/telephone order transactions
   Are out of scope

5. Merchant-initiated transactions
   Typically recurring payments by agreement between the cardholder and merchant. Once agreed, merchants may initiate subsequent payments without SCA from the cardholder. If the mandate to start these transactions is provided through a remote channel, SCA applies to the set-up/first transaction.

6. One leg out transactions
   When either the card issuer or acquirer are located outside the European Economic Area (EEA) e.g. a shopper using a Chinese-issued card at an EEA e-commerce retailer.

7. Secure corporate payments
   made through dedicated corporate processes and protocols, e.g. lodge cards, central travel accounts and virtual cards.

8. Transaction risk analysis (TRA)
   Where effective risk analysis tools are in place such that fraud rates remain within certain strictly monitored parameters.

9. Transport fares or parking
   At unattended devices (e.g. fare gates and parking meters) are out of scope.

10. Trusted beneficiaries
    Added by the cardholder to a list of trusted beneficiaries held by their card issuer, sometimes also known as ‘white-listing’.

Regulators hope that the new requirements will protect consumers, drive the digital agenda, competition and security across Europe.

pxp

What happens if you ignore the deadline and do nothing?

The short answer is you will experience higher than usual declines. From 31 December 2020 in Europe and 14 March 2021 in the UK, issuers will start declining all transactions that go straight to authorisation (i.e. do not request authentication or invoke an exemption). Those who have not updated their process flows, may also miss out on some of the functionality within the new 3DS 2.0 protocol for frictionless flows. For example, the ability to pass more data to issuers for better risk scoring, and optimise the check-out flow for shoppers on mobiles, tablets and in-app.

What happens after the deadline?

EEA Card Issuers are required by law to soft decline (Where they request you to perform 3D Secure before re-attempting the transaction) any in-scope ecommerce transactions that have not been successfully authenticated via 3D Secure, unless an appropriate exemption has explicitly been requested and accepted at the time of authorisation. This ultimately means the merchant will no longer be able to accept ecommerce card payments without 3D Secure or exemptions.

How does PXP provide merchants with a solution to comply with the regulations and continue trading online?

PXP's ANYpay gateway already supports both 3DS 1.0 and 3DS 2.0 and is certified with the main international card schemes to that end. This means we can automatically use the 3DS version supported by the cardholder's issuer. We can also automatically render the authentication pop-up window for the cardholder's device to help make the authentication process as smooth as possible. We have devised four strong customer authentication policies for processing online payments to suit all merchants, sectors and geographies and are working with merchants on implementing them in the way that best fits their trading patterns and customer base.

Policy & Description

1.	Apply strong customer authentication only when both the card issuer and acquirer are located within the EEA, using the 3DS version supported by the card issuer. SCA exemptions to be applied by PXP where possible. Default unless otherwise specified
2.	Apply strong customer authentication on all payments regardless of where the card issuer is located, using 3DS 2.0. If strong customer authentication is mandated but 3DS 2.0 is not supported by the card issuer, then use 3DS 1.0. SCA exemptions to be applied by PXP where possible.
3.	Apply strong customer authentication on all payments regardless of where the card issuer is located, using the 3DS version support by the card issuer. SCA exemptions to be applied by PXP where possible.
4.	Do not apply strong customer authentication.

For more information on the policies, please visit: https://developer.pxp-solutions.com/reference#sca-policy. Our ANYpay online developer hub also contains various integration guides, API references, examples and test scripts and is publicly available at https://developer.pxp-solutions.com.

pxp


pxp