barclaycard
Start today

Demystifying the payment landscape

PSD2, SCA and the security challenge

Introduction

This whitepaper traces the origins and impact of the second Payment Services Directive (PSD2) and Strong Customer Authentication (SCA). It examines how new technology and regulations are shaping the payments industry, and what this will mean for everyone in the payments chain.

We look at the rise of fraud and review the authentication requirements and exemptions under SCA. And we show typical payment journeys in different eCommerce situations so that merchants have a clearer understanding of how payments are changing, and will continue to change, when PSD2 SCA is introduced later this year.

David Jeffrey

Director of Fraud, Security and Optimisation, Barclaycard Payment Solutions

Jasmine Wu

Strategy Manager, Barclaycard Payment Solutions

Muhammad Shoaib Shahid

Product Manager, Fraud and Security, Barclaycard Payment Solutions

Contents

Executive summary

The global payments industry is going through unprecedented change. Technology is redefining what banking means, how financial services are delivered and by whom.

The financial world is now digital, mobile, cross-border, increasingly connected and omnichannel, paving the way for new payment methods that meet the needs of consumers who expect frictionless transactions.

Securing the future

While technology is taking speed and convenience to new heights, it is also enabling cybercrime. A global 2018 study by PwC revealed that 49% of organisations admitted to being victims of fraud, up from 36% in 2016[1]. The rise accompanies the growth in card-not-present (CNP) transactions, now the primary payment method for eCommerce sales across the globe[2].

Payment service providers, merchants and regulators face the challenge of reinforcing eCommerce security, without creating obstacles that could lead to cart abandonment. Much has happened in the decade since the first Payment Services Directive (PSD1) was introduced. Fraud losses have risen year-on-year against a background of rapid digital change, with open banking and FinTechs radically disrupting traditional payment methods.

Stronger authentication

The second directive, PSD2, is a response to these changes, bringing regulations and security measures up to date with SCA.

The main objective of SCA is to make European online payments far more secure. From 14 September 2019, all eCommerce transactions (within certain categories and values) must be authenticated in line with the new Regulatory Technical Standards (RTS).

These standards provide the framework for SCA. With only months to go, payment service providers must assess their requirements and ensure that the right systems and procedures are in place to be compliant.

[1] https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
[2] https://financeandriskblog.accenture.com/cyber-risk/finance-and-risk/the-scope-of-the-card-not-present-cnp-fraud-problem

Helping merchants make the change

SCA will have a significant impact on merchants, and a key recommendation is that closer partnerships are required across the payments chain.

Merchant agreements and card scheme rules must be revised to conform with SCA. Merchants are likely to seek support from payment service providers who can dynamically optimise payment journeys.

In preparation for SCA, there have been numerous consultations about the application and scope of authentication, and further refinements are likely before SCA is rolled out. Exemption applications, for example, may vary across different industries, acquirers or countries.

Although some uncertainties remain, there are clear priorities for merchants:

- Get ready for 3-D Secure version 2 (3DS2), the security infrastructure for SCA
- Consider how fraud solutions can strengthen access to exemptions and manage liability exposure
- Assess payment journeys, operating models and the changes that are needed
- Optimise the use of agreed exemptions
- Collaborate to find solutions.

Barclaycard in the new payments world

From the time SCA was announced, Barclaycard has been strongly involved in industry-wide discussions about the application and implementation of the directive. We encourage merchants to understand how SCA will impact their customer journeys and sales models.

Our aim is to achieve a balance between managing risks and maintaining the speed and convenience that payment technology provides – and customers now expect.

Section 1: PSD2 and the road to SCA

PSD2 is a big step forward for security and has many interlocking elements. Here's how the pieces come together.

A new digital frontier

The regulatory environment for European payments is complex and constantly evolving. New mandates and protocols emerge every year – creating a host of new abbreviations and acronyms – while security is constantly playing catch up with sophisticated fraudsters and the vast amounts of data generated every day.

SCA is designed to tackle the rising levels of online fraud and safeguard data. eCommerce – and now especially mobile commerce – is a prime target for fraudsters. In 2012, £140m was lost to eCommerce fraud in the UK alone. By 2017, the figure had more than doubled.[3]

While most people agree that we need stronger measures to prevent online fraud, some feel that heightened security may have a negative effect on the shopping experience and impact sales through cart abandonment – which, of course, is another form of loss.

This is the challenge that payment service providers face in implementing the requirements of PSD2. Moreover, it's been a long journey and many steps remain.

[3] https://www.ukfinance.org.uk/data-and-research/data/fraud

Where did PSD2 come from and where's it going?

PSD2 was officially published by the European Commission at the end of 2015. It followed the first Payment Services Directive (PSD1), which was introduced in 2009 and created the legal framework for SEPA (Single Euro Payments Area).

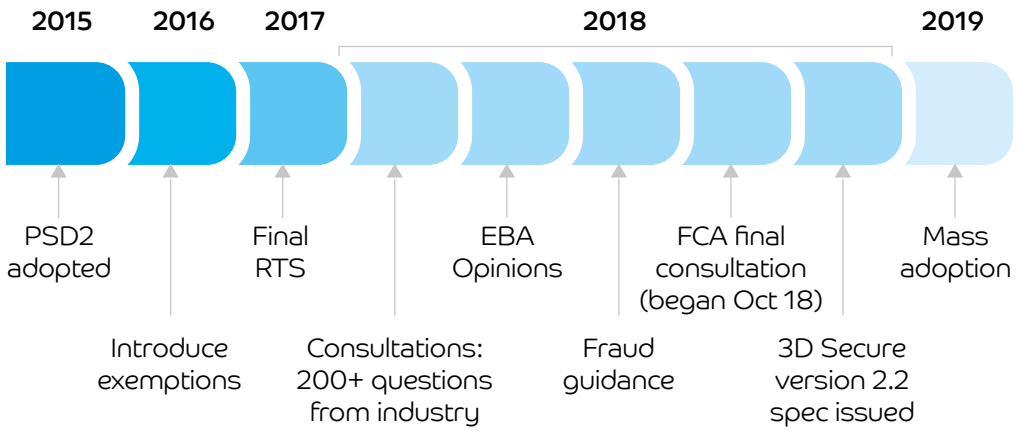
PSD2 was implemented in January 2018 and applies to all companies in the European Economic Area (EEA) that deal with payments. In addition to this year's 14 September deadline, by which time the technical standards for SCA must be implemented, all application programming interfaces (APIs) must be ready by March. These are the open interfaces that payment service providers need to comply with SCA. The API technical specifications must be published and be publicly available, and testing facilities are also required.

Cash is no longer king

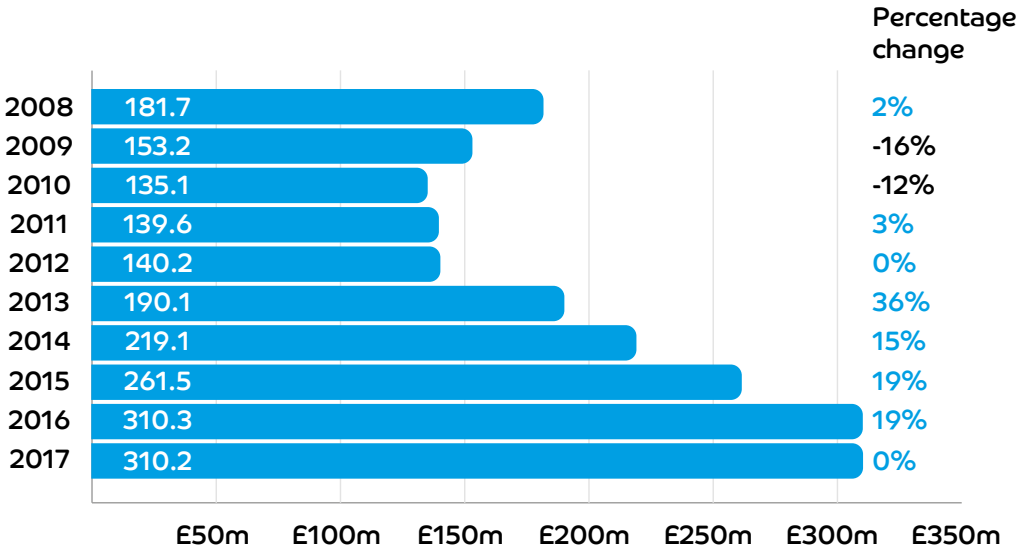
Since PSD1 was first implemented, eCommerce has boomed across Europe, while huge advances in digital and mobile transactions have bought greater speed and convenience to shoppers. The scope of the original directive has been overtaken by technology, with third-party providers continually developing new payment channels (and fraudsters busily finding ways to exploit them).

According to a 2017 research report from Visa, 77% of Europeans now use their phones to bank and make everyday payments[4]. One thing is certain: online shopping will only increase, and so will the opportunities for fraud.

PSD2 Timeline



Internet/eCommerce fraud losses on UK-issued cards 2008-2017[5]



[4] https://www.visaeurope.com/newsroom/news/mobile-money-takes-off-as-77-of-europeans-use-their-phones-to-bank-and-make-everyday-payments
[5] UK Finance, 2018 https://www.ukfinance.org.uk/data-and-research/data/fraud

Who's in control with PSD2?

Security is just one of the priorities for PSD2. The directive includes 112 articles and mandates on a range of topics that regulators asked the European Banking Association to examine. Along with increased security, the broad aim is to open the field to new payment service providers and promote competition and innovation.

Banks are now required to offer their APIs to third parties who will then be able to access customers' data (with their consent) and develop new financial offerings. This means that non-banks can move into the traditional banking space and, among other things, make payments on behalf of customers.

Because much attention has been given to the democratising effect of PSD2, some observers view it as a free-for-all that places customer data at risk. What, they ask, will happen when banks are no longer in control?

Moreover, by opening up customer information to third parties, some believe that PSD2 conflicts with GDPR (General Data Protection Regulation), the other major directive introduced in 2018. Whereas GDPR assumes the right to privacy and significantly restricts the way data can be held and used, PSD2 implies greater data freedom. However, this ignores the controls provided by SCA, which prioritise customer security and are complementary to GDPR.

The new payment players

PSD2 creates two main types of players who will take advantage of banks' open APIs:

- Payment Initiation Service Providers (PISP) – these are providers who can initiate payments on behalf of a consumer. They can withdraw money directly from your account with your consent.

- Account Information Service Providers (AISP) – AISPs have access to the account information of bank customers. Access can lead to services such as analysing a user's spending behaviour or consolidating a user's account information from several banks.

3-D Secure

Current authentication practices are based on 3-D Secure (3DS), which stands for three-domain secure. The three domains are:

- Merchant acquirer domain
- Issuer domain
- Network domain (i.e. the payment system).

Introduced in 1999, 3DS is a messaging protocol developed by EMVCo, the organisation responsible for developing the Eurocard, Mastercard and Visa specifications. Most people who have shopped online will be familiar with the first version (3DS1), which enables consumers to authenticate themselves with their card issuer when they make card-not-present purchases.

3DS1 is the password protection that you encounter when completing a transaction, and it involves being redirected to a new page where you must input a code. In other words, information to authenticate yourself.

There are several drawbacks with this first version, not least a dependency on pop-up windows which are difficult to distinguish from phishing sites because the windows are served from a domain that cannot be verified. In addition, mobile browsers can be a stumbling block because they often lack pop-up functionality. In short, 3DS1 is unsuitable for today's eCommerce transactions.

The protocol belongs to a different age and has generally been viewed as detrimental to customer experience (and one of the main reasons for cart abandonment and poor conversion rates). It has also suffered internationally because of the way payments are processed in different markets. Legal frameworks and security requirements vary from country to country and bank to bank, which means adoption has been patchy at best.

For these and other reasons, 3DS1 is not an appropriate foundation for PSD2. The solution is version 2 of the protocol, 3DS2, which provides the right technology infrastructure for strong customer authentication in the mobile era.

3-D Secure 2.0

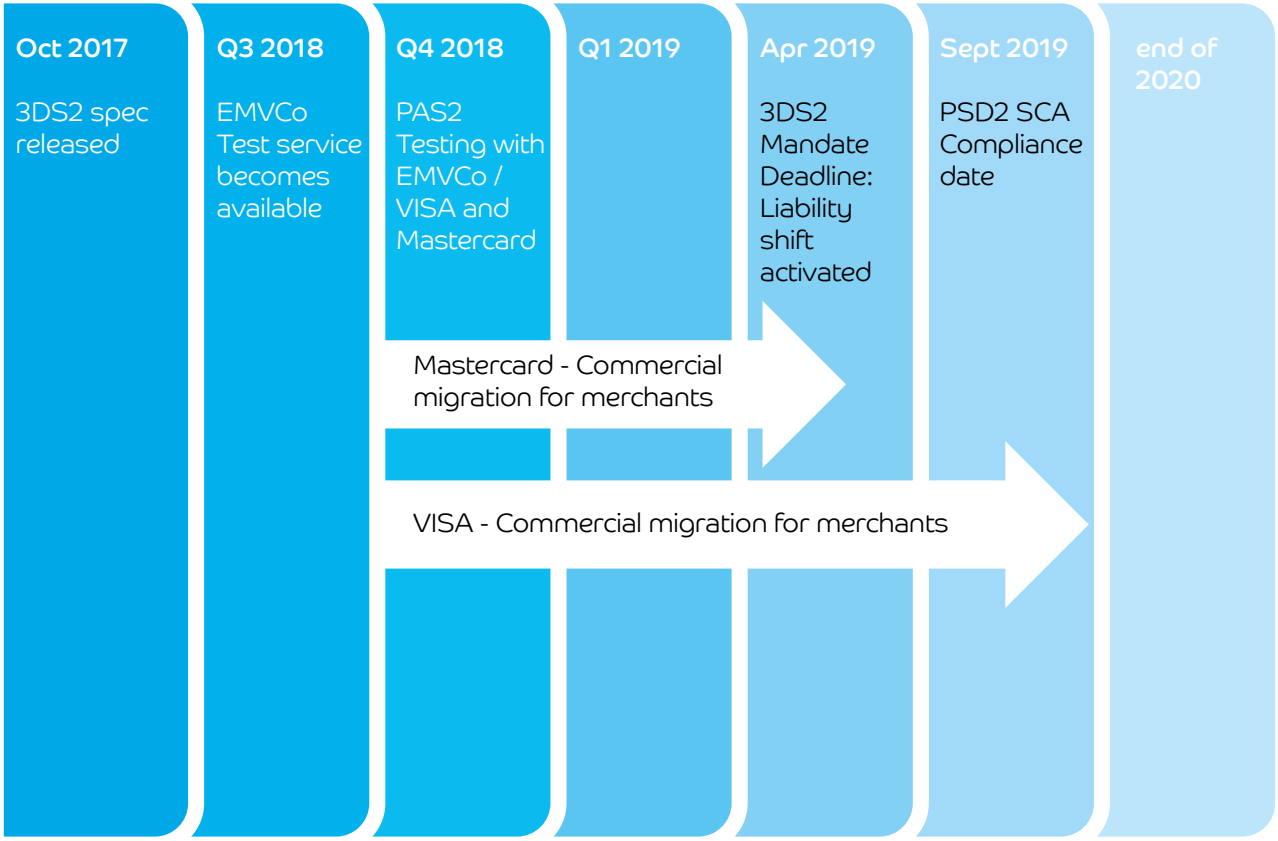
The updated version of the protocol represents a new approach to security – one that's in keeping with today's online and mobile world and is based on a wider range of data. It eliminates some of the challenges of 3DS1, and strengthens the ability to meet Regulatory Technical Standards (RTS). The standards were issued by the European Banking Authority and provide guidance on what constitutes strong customer authentication.

The advantages of 3DS2 over 3DS1 include:

- Far more data points to help verify transactions
- Better risk-based authentication
- Better performance for end-to-end message processing
- Integration of the authentication process into merchant checkout experiences, both for app and browser-based implementations (eliminating the redirect issue with 3DS1).

3DS2 is scheduled to be in place for issuers and acquirer/gateways by April 2019, ready for the arrival of SCA in September 2019.

3DS2 Timeline



Section 2: SCA in practice

What are the requirements for strong customer authentication, how will they impact purchasing, and what are the exemptions?

Changing the rules

3DS2 provides the rails for merchants to flow a much larger range of optional data points in the authentication process, which will likely result in better and more positive decision making from issuers. With 3DS2 set to be mandatory from April 2019, the payments industry will have an up-to-date infrastructure to apply SCA. And because the protocol generates over 100 data points to help determine the validity of a transaction, payments will be more secure than with simple password authentication.

SCA applies to customer-initiated online transactions over €30; however, SCA is also required if there have been five exempted transactions or the sum of exempted transactions exceeds €150.

Although SCA applies only to transactions in the European Economic Area (EEA), where both the issuer and acquirer are in the region, the principle of 'best endeavours' should be followed when one of the parties is outside the EEA. Most card payments and all credit transfers will require SCA.

Two-factor authentication

SCA is predicated on a two-factor principle, which means that authentication will require two out of three possible security checks. Namely: 'something you know', 'something you are', and 'something you have'.

'Something you know' is the familiar username/password approach, while 'something you are' adds biometrics to the verification process. A phone or a card would be an example of 'something you have'.

The inclusion of biometrics, such as fingerprint or iris recognition, reflects the realities of mobile communication and the need to make mCommerce as seamless as possible.

Something you own:

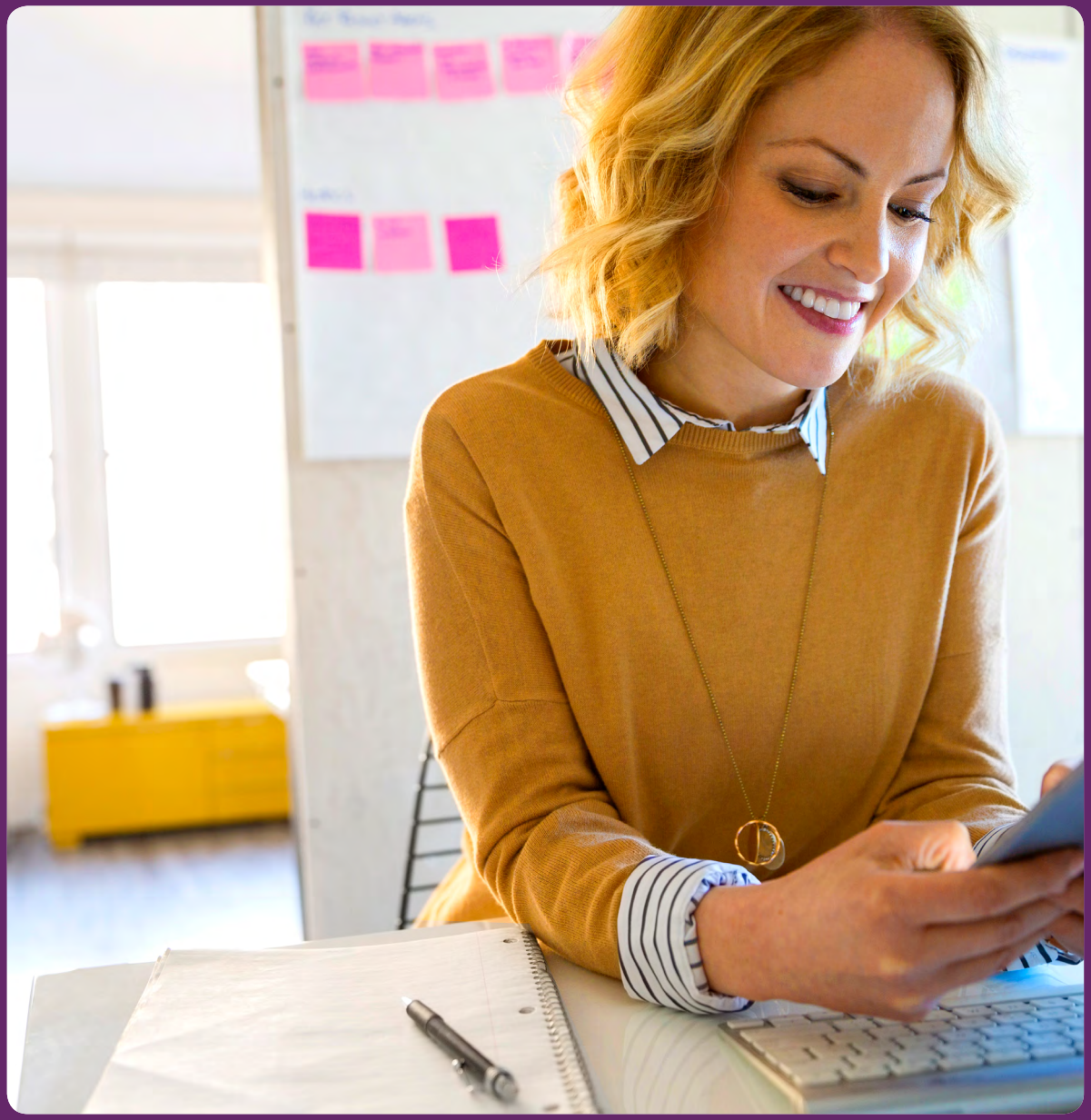
- Mobile phone
- Wearable device
- Smart card
- Token
- Badge

Something you know:

- Password
- Passphrase
- PIN
- Sequence
- Secret question

Something you are:

- Fingerprint
- Facial recognition
- Voice patterns
- Iris scan
- Keystroke analysis



Frictionless flow versus fraud prevention

SCA has many implications for transaction processing and customer experience. One advantage is that shoppers no longer have to negotiate pop-up windows, while biometric recognition is a swift, secure, and far more practical solution for mCommerce. Few would dispute the benefits of self-authentication through the tap of a finger or facial recognition.

However, what will two-factor authentication mean in reality? Will the additional security requirements complicate the shopping experience? When the move to 3DS2 was first discussed, there were fears that every transaction would need to be challenged, creating frustration, delays, and abandoned purchases.

But this is not the case. SCA balances the need for frictionless flows with the need for strong security. The application of SCA is therefore a matter of interpretation, with merchants being allowed to offer frictionless flow according to, for example, the value of the purchase and the fraud rate of the acquirer and the issuer.

Exemptions

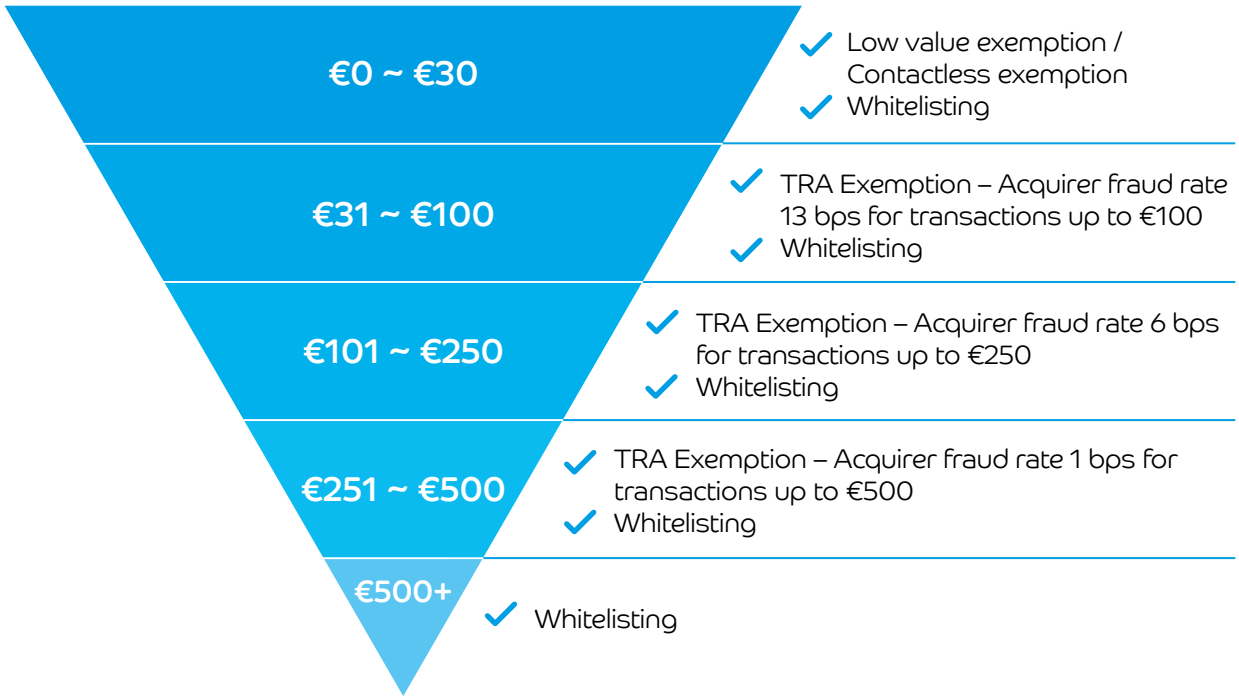
The goal is to increase security but without being overly restrictive. Note that issuers (i.e. the banks that provide payment cards to consumers on behalf of card networks) always have the final say, and merchants cannot apply exemptions, although acquirers can on their behalf – but only if the issuer agrees with the exemption.

In addition to exemptions, the following are automatically classed as 'out of scope' and not subject to SCA:

- Mail order and telephone order transactions (known as MOTO)
- Merchant-initiated transactions (provided conditions are met)
- 'One leg out' transactions (where either the issuer or acquirer is outside the EEA). SCA is required only on a 'best endeavours' basis
- Anonymous payments.

What exemptions are available at each tier?

The higher the transaction value, the less access to exemption



Structured transactions (e.g. recurring exemption or secure corporate payments) – not restricted by transaction values

Here are the principal exemptions:

Low value transactions

Card transactions below €30 are deemed low value and normally exempt from authentication. However, SCA will be required if the customer initiates more than five consecutive low value payments or if the accumulated payment value exceeds €100.

Recurring payments such as subscriptions

Recurring payments of the same value to the same merchant are exempt, but they will require SCA for the initial set up. Not exempt: periodic payments to the same payee where the value changes each time (e.g. a utility bill), but there is some debate whether this would apply under merchant-initiated transactions.

Whitelisting

Customers can 'whitelist' trusted merchants. This means flagging them as 'trusted beneficiaries' who do not require authentication once an initial check has been made. Issuers are the custodians of the whitelist and may set their own eligibility criteria.

Secure corporate payments

If a transaction is initiated by a legal entity (e.g. a business) rather than a consumer, and the transaction is processed through a secure payment protocol, it will not require separate authentication if the alternative controls are secure.

How do the exemptions work?

Exemption example: Whitelisting

Customers can elect to whitelist a merchant they trust with their issuer:

- Once whitelisted, subsequent transactions are exempt
- Only Issuer has control over the list
- Adding, amending or deleting require SCA
- Merchants cannot maintain the list for this purpose

A typical whitelisting transaction

This would not be the only way to 'whitelist' a merchant. Industry is working on all the potentials, as well as rules of the road for the application.

Transaction risk analysis (TRA)

An exemption might apply if a transaction is deemed to be low risk. This is a complex area with many criteria that require careful scrutiny. For example, risk assessments may be based on geolocation data or behaviour patterns.

The fraud rate of the acquirer is key in determining whether TRA can be applied. Even if an acquirer has a poor fraud rate, transactions under €30 are still exempt from SCA. If the acquirer has a fraud rate of lower than 13 basis points (bps), which is a measure of the acquirers' current fraud losses, it can use TRA for transactions with a value of €100 or less. TRA will encourage acquirers to improve their fraud rates so they can offer a more frictionless shopping experience.

The issuer always has the final say for all transactions.

Contactless

Transactions below €50 are exempt for up to five consecutive transactions or an accumulated value up to €150.

Unattended terminals

Exemptions typically apply to transport fares or parking fees.

Section 3: Conclusion

Regulations are both an opportunity and a challenge. Here are some of the ways you can turn PSD2 into a strategic advantage.

It's a beginning, not an end

PSD2 is part of a wave of regulatory reforms that will bring the financial services industry up to date with new technologies and market developments. For payments, 2019 will be a watershed year as the new EU directive takes shape and we move towards the September cutover for SCA. But it won't stop there: PSD2 must evolve to keep pace with technological transformation and disruption.

Over the last few months there have been refinements to PSD2, following clarifications from the EBA and the regulators. In December 2018, EMVco announced tweaks to the 3-D Secure specification. We now have 3DS2.2, an update that includes enhancements to optimise the consumer experience while supporting new authentication methods. The enhancements include improved communication between merchants and issuers, which should help to clarify exemptions. Future iterations of the directive are likely to address instant payments and other developments.

Testing, testing...

From 14 March, there is a three-month test phase for interfaces (ie, open APIs). One of the aims is to ensure they comply with the final Regulatory Technical Standards (RTS) on strong customer authentication. Banks and other account servicing payment service providers (ASPSPs) must provide a testing facility for third-party providers (TPPs).

Walking the line

As mCommerce expands, the success of SCA will depend on shrewd interpretation. In 2019, mobile transactions are set to exceed the volume of eCommerce for the first time globally. Consumers now expect to use handheld devices to engage and transact seamlessly with businesses, but that can't happen if there are too many security hurdles.

Clarifications from regulators will help to ensure the right balance. For example, TRA can promote a smooth purchasing experience and still ensure security, but risk levels and exemptions depend, among other things, on the tolerance of the issuer, the country of jurisdiction, and, of course, different industry requirements.

It remains to be seen how exemptions will apply and evolve after September. As mentioned on page 14, the fraud rate of the acquirer is a key factor in determining if TRA can replace SCA. As a catalyst for frictionless commerce, acquirers would do well to improve their fraud rates. Issuer fraud rates are also important, since anything less than 13 bps means that issuers can choose not to apply SCA if they deem it to be low risk.

Who's now liable?

One of the benefits for merchants is that when 3DS2 is applied, they are not liable for fraudulent transactions. Currently, when the cardholder or issuer disputes an online transaction (on the basis that it is fraudulent), in most cases merchants would refund the loss. With 3DS2, as it does today with 3DSv1, liability will shift to the card issuer/cardholder. This is illustrated in the table opposite.

Brexit: to be or not to be?

In addition to 19 September, there is another important deadline in 2019. On 29 March, the UK is due to leave the EU. While it remains unclear how the UK will approach the requirements of PSD2 following Brexit, many financial institutions are taking steps to address Brexit, and Barclaycard is no exception. Barclaycard Payment Solutions has implemented its Brexit strategy and is ready to support all its customers regardless of the political situation. Further information can be viewed at:
www.barclaycard.co.uk/business/news-and-insights/our-plans-for-brexit

From April 2019

		3DS
	Issuer / Acquirer/ Merchant: Non-secure	3DS1 & 3DS2
	Non-secure	Merchant	Merchant
3DS	3DS1* & 3DS2	Issuer	Issuer

*Visa offers liability shift for merchants attempted 3DS2

The road ahead

Barclaycard is well prepared for SCA and 3DS2. We will respond to any refinements and amendments to the payments infrastructure during 2019 and beyond, and have been working closely with clients and the payments industry while PSD2 has been rolled out. During the SCA transition period, we will help to create a balanced and practical view of fraud prevention versus frictionless flow.

We're here to offer insights and guidance so that merchants can apply new regulations in the most practical and effective way. With the right approach, the payments industry can comply with SCA and increase security without damaging consumer experience. At the same time, it can promote innovation and turn disruption into competitive advantage.

Glossary

Acquirer
Acquirers/acquiring banks process credit or debit card payments on behalf of merchants. Acquirers are registered members of card schemes (e.g. Mastercard) and acquire transactions on card networks. The network connects acquirers to issuers, enabling transactions to be verified and then either approved or declined.

AISP
Account Information Service Providers (AISPs) are businesses that can obtain a customer's account data and offer bespoke financial products and services.

API
An Application Programming Interface (API) facilitates communication between different components/software.

Cardholder
A cardholder is an individual or business that has been issued with a card to make credit/debit payments.

Card Not Present (CNP)
A card transaction where the shopper does not physically present the card. Examples include online payments, in-app payments and MOTO (mail order/ telephone order) transactions.

Chargeback
A transaction that is disputed by a cardholder or card issuer, and reverts to the merchant for resolution.

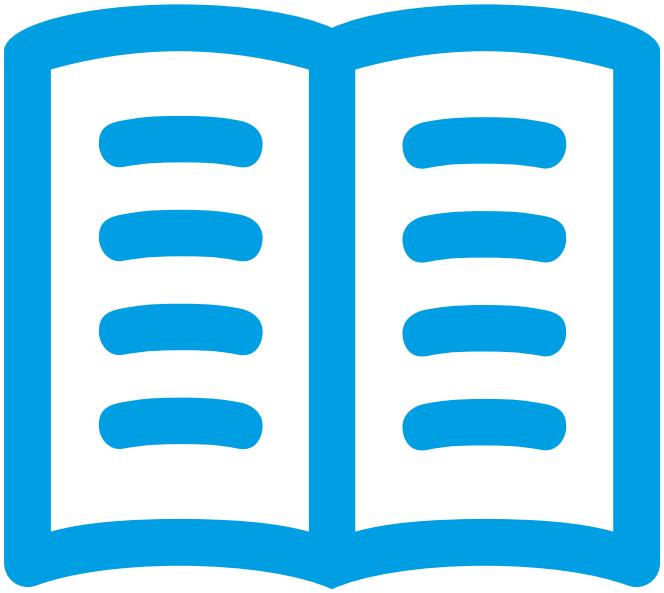
Gateway
A software link that provides the interface between merchants and acquirers.

GDPR
The EU General Data Protection Regulation (GDPR) is a law introduced in 2018 to strengthen data protection and privacy for all individuals within the European Union and the European Economic Area.

Issuer
A card issuer is a bank or financial institution that 'issues' branded payment cards to consumers.

EBA
The European Banking Authority (EBA) is an EU body that promotes effective regulation and supervision across the European banking sector.

EMVco
The company that developed the 3-D Secure solution. EMV stands for EuroPay, Mastercard and Visa.



Merchant
A retailer, or any other entity, that agrees to accept payment cards to fulfil an order for goods or services.

PISP
A Payment Initiation Service Provider (PISP) is a third-party provider that can carry out payments directly from a customer's account.

PSD2
The Payments Services Directive 2 (PSD2) is the overall payments regulation of which SCA is a part.

The 3 pillars of PSD2 are:
- Consumer Protection
- Strong Customer Authentication
- Open Banking

PSP
PSP refers to issuer and acquirer in the card payment domain.

RTS
The Regulatory Technical Standards (RTS) codify the regulatory requirements to ensure that payments across the EU are secure and efficient.

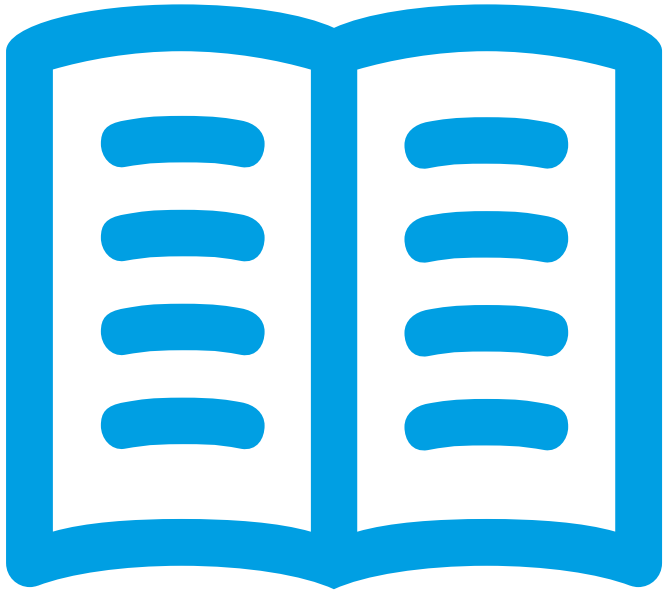
SCA
Strong Customer Authentication (SCA) is the method to authenticate who you are when making a purchase. It is mandatory under PSD2 RTS and requires at least two of three possible authentication routes:
Knowledge – something the user know
Possession – something the user has
Inherence – something the user is.

3-D Secure
A security method that prevents fraud during online payments. 3DS2 brings a new approach to authentication through a wider range of data and the addition of biometric authentication.

SEPA
The Single Euro Payments Area (SEPA). The aims of SEPA are to make it easier to transfer money and electronic payments between the member countries.

TPP
A third-party provider (TPP) is the collective name for AISPs and PISPs.

TRA
Transaction Risk Analysis (TRA) is one of the SCA exemptions that will support frictionless flow.



barclaycard
Start today

Find out more at
barclaycard.co.uk/corporate-payments

Call us on 0800 056 1242
Monday – Friday, 9am-5pm