globalpayments

# The changing face of card payments

## Your guide to the EU Payment Services Directive (PSD2) and Strong Customer Authentication (SCA)

*Service. Driven. Commerce*

# Table of contents

# Background

*Nick Corrigan, UK/I President and Managing Director*

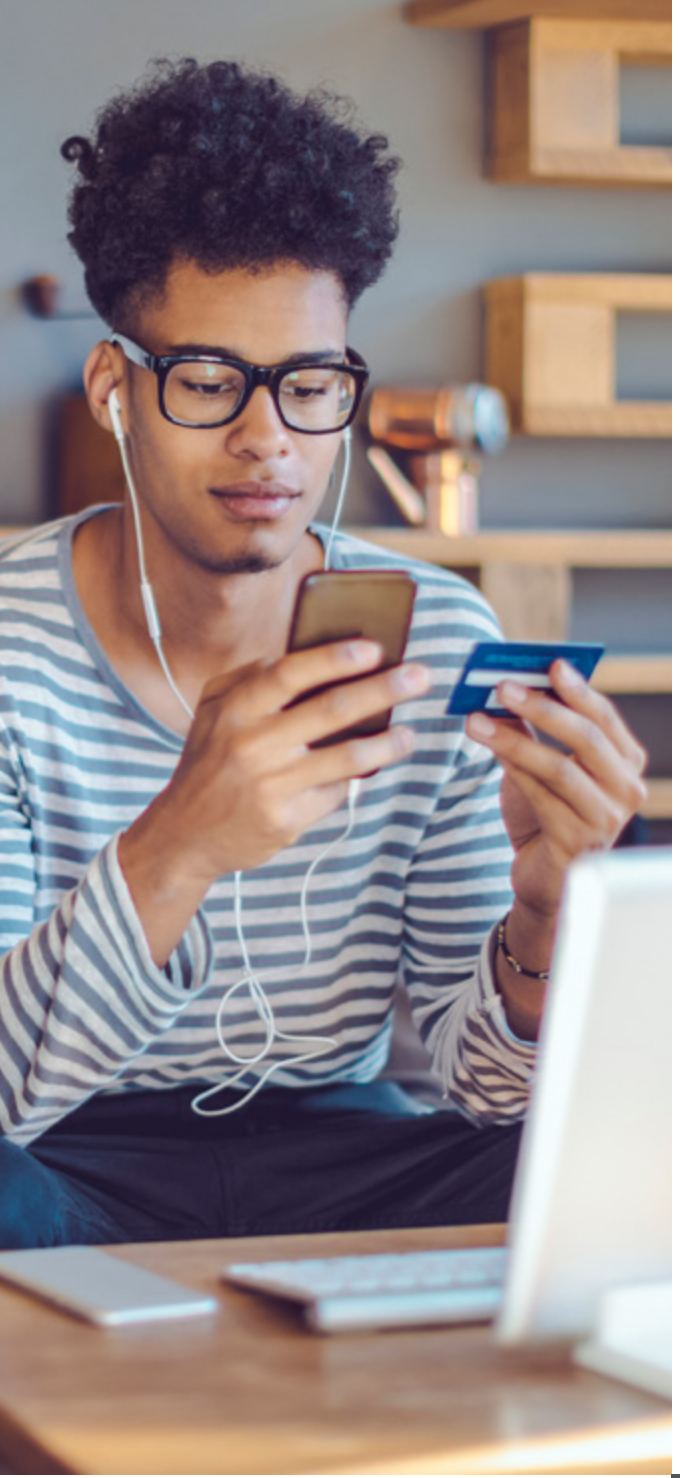
**The European payments industry is undergoing a period of huge transformation. Increasing customer expectations, new financial regulations and nimble fintech start-ups are disrupting the status quo, requiring companies of every size to reshape their business models and get ready for changing tides.**

We believe that these changes can be a good thing. Advances in both technology and customer expectation creates an opportunity to innovate and differentiate from the competition. It enables businesses to build stronger relationships with their customers and deliver the exact service they're looking for.

One significant change for the industry is that in January 2018, the European Payment Services Directive (PSD2) took effect and with it introduced new laws aimed at reducing online fraud and protecting consumer rights. Subsequently, an important element of PSD2 is the introduction of Strong Customer Authentication (SCA) on 14 September 2019 for in-store and online transactions.

Here at Global Payments, we see PSD2 and SCA as an opportunity for the market to embrace additional levels of security and use it to educate customers on the importance of strong authentication when making payments in-store, online or in-app.

To take you through the changes step by step we've created this guide to answer key questions around PSD2 and SCA.



# Taking stock of today's payments industry

**Thanks to advances in technology, the way we shop and pay has transformed at an astronomical rate in the last two decades – all designed to bring more speed and convenience to the customer. In fact, over three quarters of Europeans now use mobile devices to keep track of finances and to make payments, compared with just 18% in 2015[1].**

This demand creates a need for merchants to meet these expectations and deliver a fast, simple and secure form of payment, regardless of whether this is in-store or online. If they don't, the danger is that customers will become frustrated and take their business elsewhere.

The online checkout process, coupled with difficulties with inputting credit or debit card information, can have a knock-on effect on a company's sales.

**Approximately US$200 billion (*£158 billion) in sales are lost each year due to this friction with payment[2].**

1. https://www.jpmorgan.com/europe/merchant-services/strong-customer-authentication referencing statistics from:
   Visa Europe. 'Mobile Money Takes Off as 77% of Europeans Use their Phones to Bank and Make Everyday Payments.'
   Available at: https://www.visaeurope.com/newsroom/news/mobile-money-takes-off-as-77-of-europeans-use-their-phones-to-bank-and-make-everyday-payments Accessed October 2017.
   Visa Europe. 'Mobile Payments soar as Europe embraces new ways to pay.' Available at: https://www.visaeurope.com/newsroom/news/mobile-payments-soar Accessed October 2017.

2. https://www.pymnts.com/checkout-conversion/2018/ecommerce-friction-2017/

## Fraud Volumes by Fraud Type

| Fraud Type[5] | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | % Change 17/18 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Remote Purchase (CNP) | 266.4 | 226.9 | 221.0 | 247.3 | 301.0 | 331.5 | 398.4 | 432.3 | 408.4 | 506.4 | 24% |
| Of which e-commerce | 153.2 | 135.1 | 139.6 | 140.2 | 190.1 | 219.1 | 261.5 | 310.3 | 310.4 | 393.4 | 27% |
| Counterfeit | 80.9 | 47.6 | 36.1 | 42.3 | 43.3 | 47.8 | 45.7 | 36.9 | 24.2 | 16.3 | -33% |
| Lost & Stolen | 47.2 | 44.2 | 50.1 | 55.4 | 58.9 | 59.7 | 74.1 | 96.3 | 92.9 | 95.1 | 2% |
| Card ID Theft | 38.1 | 38.1 | 22.5 | 32.6 | 36.7 | 30.0 | 38.2 | 40.0 | 29.8 | 47.3 | 59% |
| Card not-received | 6.9 | 8.4 | 11.3 | 12.8 | 10.4 | 10.1 | 11.7 | 12.5 | 10.2 | 6.3 | -38% |
| **TOTAL** | **439.5** | **365.2** | **341** | **390.4** | **450.2** | **479.1** | **568.1** | **618.1** | **565.4** | **671.4** | **19%** |
| UK | 316.8 | 271.4 | 260.9 | 288.4 | 328.2 | 328.7 | 379.7 | 417.9 | 407.5 | 496.6 | 22% |
| Fraud Abroad | 122.6 | 93.9 | 80.0 | 102.0 | 122.0 | 150.3 | 188.4 | 200.1 | 158.0 | 174.8 | 11% |

Figures in this table are volumes. Due to the rounding of figures, the sum of separate items may differ from the totals shown. E-commerce figures are estimated.

Source: UK Finance

**It's against this backdrop that the European Union is incorporating SCA as a requirement of PSD2 in September 2019 to enhance consumer protection.**

In recent years, the payments industry has worked hard to remove fraud from the face-to-face transaction environment. At the same time, fraud in the online arena has been increasing. **The total value of online fraudulent transactions amounted to €1.32 billion (*£1.2 billion) in 2016[3], compared to just €13.6 million (*£12.1 million) in 1984[4].**

This online fraud is impacting the customer experience too. According to Visa Inc., 72% of British online shoppers have abandoned their shopping baskets on retailer websites and apps due to finding the payment process tedious or concerns over online security. The payments industry takes all types of fraud very seriously and is currently working hard to ensure online transactions are secure.

To combat online fraud, the European Union passed a directive in November 2015. This came into force in January 2018 to regulate payment service providers, as well as generate competition and create new payment options. One of the goals of PDS2 is to make payments in Europe even safer for customers by ensuring that far more stringent checks are made on a person's identity when they're making a transaction.

3. https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html
4. https://www.jpmorgan.com/europe/merchant-services/strong-customer-authentication
5. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019

* GBP values calculated at currency exchange rates from June 1st 2019.

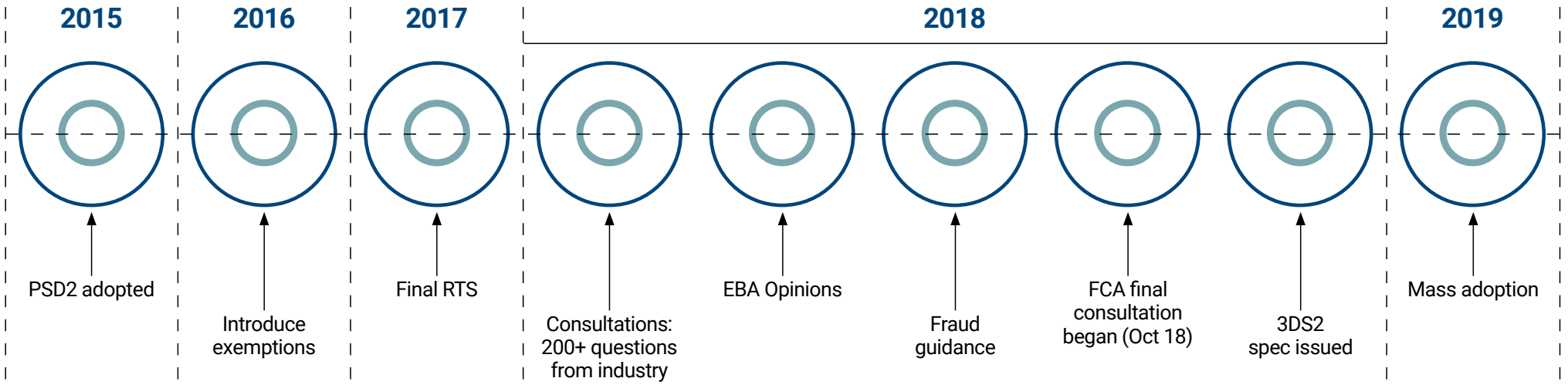
# PSD2 and the introduction of SCA

**PSD2 is a fundamental piece of payments related legislation in the EU, which entered into force in January 2018. It aims to increase competition in an already competitive industry, bring into scope new types of payment services and to enhance customer protection and security.**

When it comes to processing card payments, PSD2 mandates that all electronic payments, whether face-to-face or remote, must be completed using Strong Customer Authentication (SCA). This is a requirement in all EU countries from 14 September 2019.

If merchants are not SCA compliant then card issuers may be obliged to decline certain ecommerce transactions. In turn many businesses could see a spike in card declines if they don't put the right measures in place now.

## PSD2 Timeline



# What is Strong Customer Authentication (SCA)?

SCA is the method of authenticating an individual based on at least two discrete elements of the following three categories:

**Possession – Something only you have.**
For example, your mobile device registered with your issuing bank or a hardware token that has been issued to you.

**Inherence – Something only you are.**
For example, your fingerprint, iris scan or other form of biometric that can uniquely identify you.

**Knowledge – Something only you know.**
For example, a unique passphrase or identification number that is known only by you.

When deployed correctly, SCA offers an opportunity to keep user accounts safe, reducing the incidence of online identity theft or account takeover.

Under PSD2, card issuers are obliged to challenge and potentially decline non SCA transactions to protect their customers. Consequently, all merchants will be affected in some way to a greater or lesser extent.

# Getting ready for Compliance with SCA

## Validating in-store transactions

At the simplest level a chip and PIN transaction in a store already adheres to SCA, yet a Contactless transaction doesn't.

However, Contactless cards in a face-to-face environment are exempt from SCA if the payment meets certain parameters. The card issuer is obliged to monitor spending, and when a threshold has been reached, the customer will need to perform a chip and PIN transaction.

The regulators acknowledge that in some circumstances it may not be possible for all terminals to support SCA or have PIN pads to enter a PIN. For example, some parking meters or unattended vending machines.

## What do I need to do?

- Ensure that you and your staff understand what's happening and be ready to reassure your customer there's no problem with their card or their account, just that it's an extra security check requested by their card issuer.
- If you rent your terminals from Global Payments, you don't need to do anything to be ready for SCA.
- If you own your own terminal or rent it from another supplier, then you need to contact the provider and check requirements.

## Managing online card payments under Strong Customer Authentication (SCA)

When SCA comes into effect on 14 September 2019, all ecommerce transactions will need to adhere to the requirements. Merchants that haven't adequately authenticated their customers, (or given an adequate reason as to why they haven't or can't) will run the substantial risk that card issuers will decline their transactions.

At a minimum, you need to support 3D Secure 1 (3DS1), although we do recommend the benefits of 3DS2, with it's enhanced cardholder authentication data. If you don't, contact your payment service provider urgently and ensure that you can submit 3DS authentication requests before 14 September 2019. If you're not satisfied with your payment service provider, please contact us here at Global Payments as our 3DS1 and 3DS2 solutions will ensure that you're protected.

If you are a new customer, please ring **0800 731 8921***
Existing customers, please ring **0345 702 3344****

Or visit our website: **www.globalpaymentsinc.com/en-gb**

Ecommerce transactions have various potential exemptions that can be used. It will typically apply to transactions that are considered low-risk such as smaller payments up to £30. However, it's important to understand that if you request an SCA exemption you will be liable for any losses should they arise. Card issuers can also apply exemptions and take on the liability as this is currently how many issuers operate, performing risk based analysis and taking liability for transactions that haven't been challenged.

Launched in 2001, 3DS1 involves the following two-step process to authenticate the customer:

**1.)** Entering their card details online to confirm a payment.

**2.)** Being redirected to an in-line window where their card issuer asks them for: **a code or password to approve the purchase.**

Post September 2019, for ecommerce transactions, to allow 3DS1 to meet the basic criteria to support SCA, the current static password will be replaced with a One Time Password (OTP) sent to the customer, by their card issuer using either text or email.

*Lines are open from 9am to 5pm, Monday to Friday, except public holidays.
**Lines are open from 9am to 6pm, Monday to Friday, except public holidays, calls may be recorded.
We also provide a Textphone service on 0345 602 4818.

# 3DS2 – a new and improved solution for ecommerce

Although 3DS1 meets the requirements of Strong Customer Authentiction (SCA), it can cause some friction in today's online payments environment. For example, if the in-line window takes too long or doesn't load properly, customers are likely to abandon the purchase completely.

Additionally, many card issuers require customers to create and remember their own passwords to complete the process. With people requiring multiple passwords for lots of different accounts, these passwords are easy to forget and again can lead people to abandon the transaction.

Keen to address the challenges with 3DS1, EMVCo (the global payment standards body comprised of Visa, Mastercard, American Express, Discover, UnionPay, and JCB,) has introduced 3DS2.

The standardised design of 3DS2 across these major schemes allows for a unified authentication solution for ecommerce transactions. Plus, it's been developed with online and mobile experiences in mind as more people choose to purchase goods and services this way.

Now, instead of remembering a password, a customer will soon be able to authenticate their transaction using biometrics such as finger print recognition, which many mobile phones offer these days. The in-line payments window can also be removed, providing a smoother experience for mobile and digital wallet payment methods.


**Reminder**

3DS2, will eventually replace 3DS1. However, this won't be until later in 2021, so both will need to work together.

# Delivering a seamless customer experience online with 3DS2

While ensuring a smooth checkout process is important for in-store transactions, ecommerce transactions have a wider set of challenges and concerns that need to be addressed. 3DS2 has specifically been designed to deliver a smoother checkout experience across all devices, so that ecommerce merchants don't have to worry about abandonment on mobile devices – something physical merchants don't need to contend with.

To achieve this, 3DS2 incorporates frictionless flow that uses risk-based authentication to determine whether a customer should be challenged for further authentication during the checkout process.

Unlike 3DS1, risk-based authentication with 3DS2 allows card issuers to authenticate their customer without them even knowing that an authentication step took place.

However, implementing frictionless flow is dependent upon additional data being captured during the checkout process alongside transaction history data held by both card issuers and merchants. In total, there'll be 135 data elements that can be used to authenticate customers as part of the new protocol. This includes browser data, shipping address, customer's device ID and billing.

Providing this data, using 3DS2, potentially enables the card issuer to trust that the real customer is making the purchase and no further authentication, such as a One Time Password, is required from their customer.

If the transaction doesn't fall into an exemption category, the quality of data isn't high enough or not what the card issuer was expecting, customers will need to provide additional authentication via one of the following ways:

- **One Time Password:** This is sent by the card issuer to the customer's registered mobile number and is entered by the customer to demonstrate possession

- **Knowledge-based authentication:** Customers verify transactions by answering knowledge-based questions provided by the card issuer

Customers will also be able to authenticate a payment through their banking app using their fingerprint, (or even facial recognition in the future). This removes the inconvenience of having to remember multiple passwords and provides greater security for the customer. In fact, when customers use biometric verification, the check-out time has been shown to decrease by up to 85%, which reduces cart abandonment by an estimated 70%[6].

6. https://www.finextra.com/blogposting/15167/why-biometric-identification-is-the-future-for-online-payment-authorisation

## Our 3DS2 service for you

We can deliver a 3DS2 service that will provide effortless authentication for a faster checkout, improved security and increased conversion. This solution is available both as part of our payment gateway offering and as a standalone service that can be used in conjunction with your own gateway provider.

Our hosted payment solution is the simplest way for you to provide a fully PCI-DSS compliant, 3DS2 capable payment experience on your website.

**For more information and documentation visit:**
**www.globalpaymentsinc.com/en-gb/accept-payments/ecommerce/products/3d-secure**

# Your handy checklist ahead of 14 September 2019

With the September deadline fast approaching, it's important that merchants take time to review their current systems and processes to make sure that they can meet Strong Customer Authentication (SCA) requirements under PSD2.

We believe this new requirement should be embraced as an opportunity, as it can spark a wave of innovation that makes the shopping experience and payments process even better for your customers.

Our goal at Global Payments is to provide our customers with a complete payments solution that will put them at the cutting-edge of payment technology. We can help take on all the inherent complexity and provide merchants with an easy to deploy solution.

We also want to ensure our customers are fully supported when new rules and regulations come into effect, too. Here's what you can do ahead of the deadline:

- ✔ Check your website and review current payment methods
- ✔ Update payment methods so that they either handle 3DS1 at a minimum or upgrade to 3DS2
- ✔ Work with a trusted and reputable partner like Global Payments to help implement 3DS1 and/or 3DS2
- ✔ Inform customers of the changes and highlight the benefits that 3DS1 and 3DS2 provides to the online shopping experience
- ✔ If you own your own terminal or rent it from another supplier, then you need to contact the provider and check requirements

**To find out more about how we can support you, please visit our website:**

**www.globalpaymentsinc.com/en-gb**