



# A Brief Introduction

EU's revised Payment Services Directive (PSD2) is coming in place in September 2019 and is introducing the new SCA requirements.

## What is PSD2?



The Payment Services Directive (**PSD2**) is an EU legal framework for more open and secure payments within the EU/EEA community.

Its second revision from 2018 addresses the security of the EU users' bank account information in terms of remote payments and online banking where now an additional authentication step will be required to approve payments.



## Why was PSD2 created?

PSD aims to harmonise the European payment framework and help new players enter the payment market, by supporting open banking and third-party solutions.

With high mobile penetration rates and a strong shift towards digital banking services

**"80% preference rate for UK SME users. - Deloitte 2017"**

PSD opens the path to better open banking.

However, open banking would require third-party providers to access user banking information, which called for PSD's second revision to bring core changes to the way payment providers approach customer authentication.

## Key points of the upcoming PSD2 Regulation

On the 14th September this year, all payment providers within the EU/EEA will be required to apply multi-factor Secure Customer Authentication (SCA), based on the following revised multi-factor authentication criteria:



### Something the customer knows:

- x Password
- x PIN
- x Secret question

### Something the customer owns:

- x Mobile phone
- x Wearable
- x Token
- x Badge



### Something the customer has:

- x Fingerprint
- x Facial recognition
- x Voice pattern
- x Iris scan
- x DNA signature



Payment providers can no longer authenticate with only one but have to combine at least two of the methods proceed with payment.



## Exemption



Low-risk transactions up to **€500** and transactions under **€30** will be exempt from SCA.

Besides, to balance off SCA requirements with customer experience, PSD2 introduces requirements for **transaction risk analysis (TRA)**, where **payment service providers (PSPs)** observe transactional behaviour in real-time and assess the fraud risk levels, validating which transactions are 'low risk'. Such risk analysis includes monitoring for:



Abnormal payment patterns



Mobile device validation / SIM Swap



Abnormal transaction location



Malware

For more information, please contact:

JT Fraud Protection Services  
[jtglobal.com/international/contact/](http://jtglobal.com/international/contact/)

JT Group Ltd

@JT\_business

