

PSD2 & Strong Customer Authentication

What is SCA?



A new requirement under the revised Payment Services Directive (PSD2)



Requires two-factor authentication to be made for online access and payments



Means Payment Service Providers (PSPs) will have to make changes to security processes and procedures

When must SCA be used?

PSD2 requires that SCA must be used each time a client:

1. Accesses its account online
2. Initiates an electronic payment transaction
3. Carries out any action through a remote channel which may imply a risk of payment fraud or other abuses

What is Two-Factor Authentication?

Online access and payments will require at least two of the following:

- Knowledge: i.e. something only the user knows (e.g. static password, code, personal identification number)
- Possession: i.e. something only the user possesses (e.g. token, smart card, mobile)
- Inherence: i.e. something the user is (e.g. biometric characteristic, such as a fingerprint)

Are there any exceptions?

The European Banking Authority is tasked with deciding on exemptions. The list includes:

- read only access, with no display of sensitive payment data
- online payments to a payee on a trusted beneficiary list
- a series of online credit transfers with the same amount and the same payee
- online credit transfers between the client's accounts with the same PSP
- contactless payments up to set transaction and cumulative limits

Find out more

For payments news, guides, videos and more, register on [Engage](#).

Take a look at our in-depth, interactive [PSD2 tool](#).

For any advice about the world of payments and what it means for you, contact:



Emily Reid
Partner, London
T +44 20 7296 5362
emily.reid@hoganlovells.com



Jonathan Chertkow
Partner, London
T +44 20 7296 2191
jonathan.chertkow@hoganlovells.com



Roger Tym
Partner, London
T +44 20 7296 2470
rogertym@hoganlovells.com