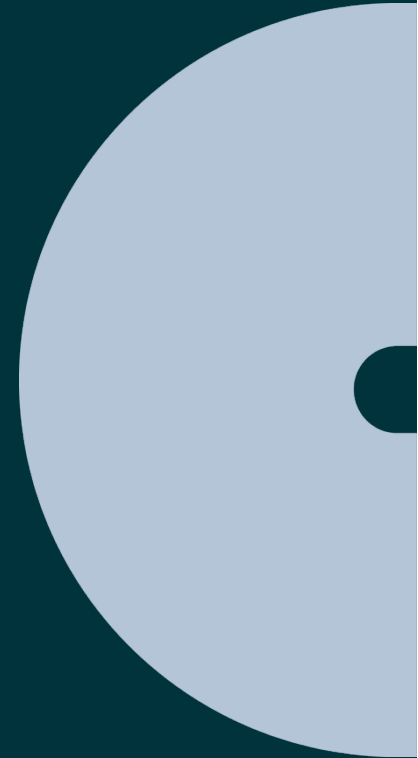
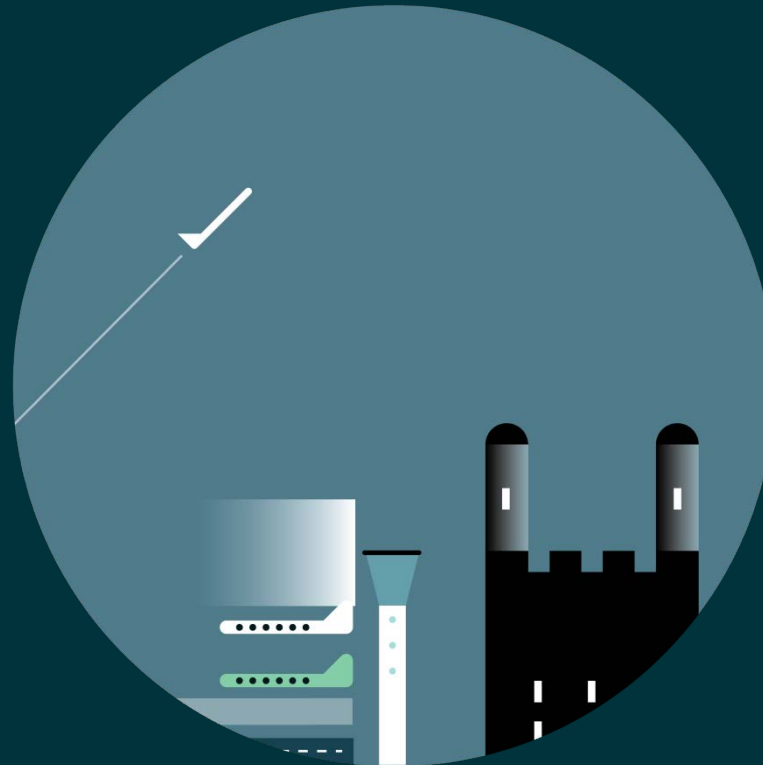


PSD2 – What is the current state of play?

Paul Anning, Osborne Clarke

22 June 2016

mobey forum



PSD2 – What is the current state of play?

Agenda

- Context
- PSD2 – Where are we now?
- 3 mobile payment specific issues under PSD2:
 - Negative scope: digital device exemption
 - Strong Customer Authentication (SCA)
 - Third Party Providers (TPPs): AIS and PIS



Context (1)

What's in a mobile payment?

- Mobile payments = payment transaction + data
- Separate regulatory regimes:
 - both are changing
 - each requires careful analysis of business and operating model
 - critical to understand regulatory responsibility
- Payment services regulatory scope:
 - can be hard to divine perimeter for all involved in a mobile payment
 - varies by model
 - expanding, e.g. under PSD2



Context (2)

More than just PSD2?

Payment services and funds transfers:

- Payment Services Directive (PSD) – PSD2, effective 13 January 2018
- Second Electronic Money Directive (2EMD)
- Cross Border Payments Regulation
- Funds Transfers Regulation – proposed revisions for 4MLD, effective 2017
- SEPA End Date Regulation
- EBA's Guidelines on the security of internet payments – effective August 2015
- Payment Accounts Directive, effective August 2016
- Interchange Fees Regulation (IFR), effective December 2015 (caps), June 2016 (business rules)

Generic:

- Fourth Anti-Money Laundering Directive (4MLD)
 - Consumer Rights Directive
 - General Data Protection Regulation
 - Proposed new Network and Information Security Directive
 - e-ID and Trust Services Regulation – effective 1 July 2016
-



PSD2

Where are we now?

- PSD2 was published in EU's OJ on 23 December 2015; entry into force 20 days after publication
 - PSD2 comes into force 2 years later, i.e. 13 January 2018
 - Subject to:
 - Transposition (i.e. implementation by individual Member States)
 - Member State derogations
 - Transitional provisions
 - EBA mandates – Guidelines, RTS (regulatory technical standards) and ITS (implementing technical standards)
-



PSD2

Negative scope: General

Exemption	Article	Recital	Commentary on scope
Commercial Agent	3(b)	(11)	Narrowed: agent can only act for payer or payee, not both
Technical service provider	3(j)	-	Narrowed: AIS and PIS excluded
Limited network	3(k)	(13) and (14)	Narrowed: e.g. "very limited" range of goods and services
Digital content/device	3(l)	(15) and (16)	Expanded: includes add to bill payments for ticket purchases and charitable donations (subject to limits)
Group	3(n)	(17)	Clarified: by additional reference to "related services"
Cash withdrawals	3(o)	(18)	Entirely new: imposes restricted set of disclosure requirements on independent ATM deployers



PSD2

Negative scope: Digital device exemption

Article 3(l):

"payment transactions by a provider of electronic communications networks or services provided in addition to electronic communication services for a subscriber to the network or service:

- (i) for purchase of digital content and voice-based services, regardless of the device used for the purchase or consumption of the digital content and charged to the related bill; or***
- (ii) performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets;***

provided that that value of any single payment transaction referred to in points (i) and (ii) does not exceed EUR 50 and: - the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month; or – where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month."

PSD2

Strong Customer Authentication (SCA)



"On the Internet, nobody knows you're a dog."

PSD2

Strong Customer Authentication (SCA) (1)

Area	Requirement
Definition	<ul style="list-style-type: none">• Requires two or more of:<ul style="list-style-type: none">• knowledge (= something only the user knows)• possession (= something only the user has)• inherence (= something the user is)• Elements must be mutually independent<ul style="list-style-type: none">• i.e. breach of one does not compromise other• Designed to protect confidentiality of authentication data
When required?	<ul style="list-style-type: none">• Payer accesses account online• Payer initiates an electronic payment• Payer carries out any action through a remote channel which may imply a risk of payment fraud /other abuse• Note: no corporate opt-out

PSD2

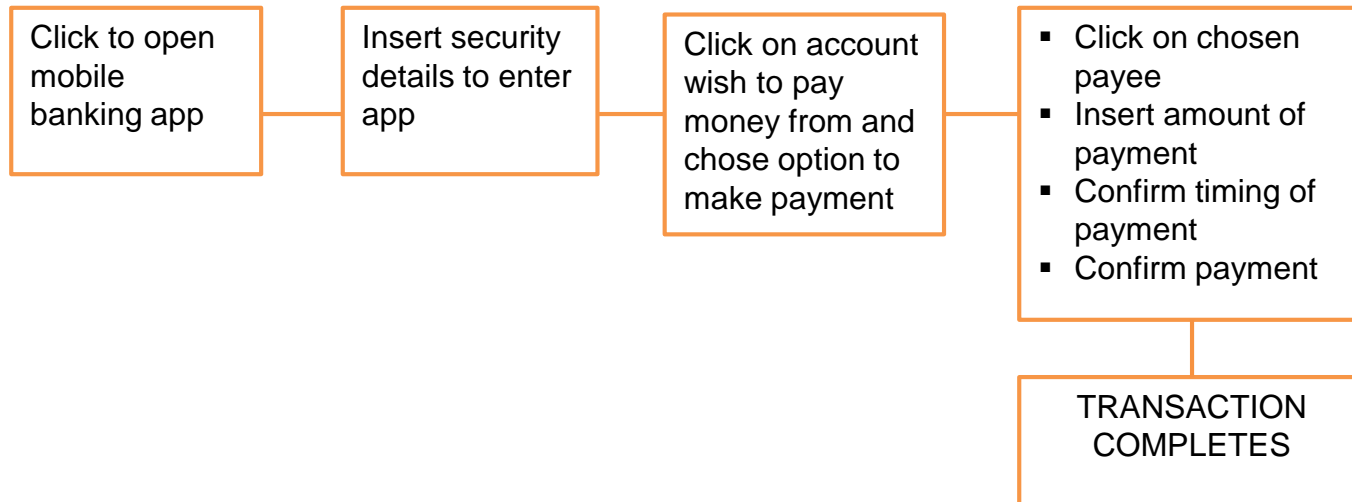
Strong Customer Authentication (SCA) (2)

Area	Requirement
Remote Payment Transactions	<ul style="list-style-type: none"> • i.e. payment transaction initiated via internet, or through a device that can be used for distance communication • For these, SCA must include elements dynamically linking transaction to specific amount and payee
Liability impact (subject to COO)	<ul style="list-style-type: none"> • If PSP doesn't require SCA, payer only liable if fraudulent • If payee's PSP doesn't accept SCA, liable to payer's PSP for unauthorised transaction
PIS and AIS TPPs	<ul style="list-style-type: none"> • Authentication requirements apply to PIS and AIS TPPs in the same way • Must be allowed to rely on authentication procedures provided by account servicing PSP to customer
Security of credentials	<ul style="list-style-type: none"> • PSPs to adopt security requirements to protect confidentiality and integrity of users' credentials

PSD2

Strong Customer Authentication (SCA) (3)

Using mobile banking app to make a credit transfer



Questions

- Is "strong customer authentication" (SCA) required?
- When should the SCA be applied?
- Does the provision of the app entry information constitute SCA?
- What are the implications of this?
- Would the credit transfer constitute a "remote payment transaction", so requiring any SCA to include elements dynamically linking the transaction to the specific amount and payee?



PSD2

Third Party Provider (TPP) services (1)



PSD2

Third Party Provider (TPP) services (2)

- Two new types of payment services added:
 - payment initiation services (PIS)
 - account information services (AIS)
 - PIS and AIS very distinct types of services
 - Technical services provider exemption adjusted accordingly
 - EC's objective is to enhance competition, encourage the digital economy and achieve harmonisation
 - Different regulatory regimes recognise very distinct types of services
-



PSD2

Third Party Provider (TPP) services (3)

- PSD2's approach is to set out rights of PSU and obligations of AS PSP and AIS/PIS TPP
 - PSU's rights include:
 - right to use an AIS/PIS TPP, where payment account is accessible online
 - right to seek compensation from his AS PSP for unauthorised payment transactions (though the AS PSP then has a right in turn to seek a remedy from the TPP unless the TPP can demonstrate that it is not liable)
-



PSD2

Third Party Provider (TPP) services (4)

- AIS/PIS TPP's obligations include:
 - act only within PSU's explicit consent
 - ensure PSU's personalised security credentials are not accessible to other parties and are transmitted only through safe and efficient channels
 - identify itself towards AS PSP every session and communicate securely
 - only seek and use data which is necessary to perform the PIS/AIS service
 - PIS TPP – not modify the transaction, nor hold the payer's funds
 - AIS TPP – not request sensitive payment data
-



PSD2

Third Party Provider (TPP) services (5)

- AS PSP's obligations include:
 - grant access, unless objectively justified
 - not discriminate payment orders received from a PIS TPP or data requests from an AIS PSP, unless objectively justified
 - provide/make available to the PIS all information on payment transaction initiation and accessible regarding execution
-



Concluding remarks

- PSD2 text settled
 - Yet much remains to be settled – application and interpretation
 - Look out for:
 - EBA RTSs
 - industry guidance
 - local implementation/transposition
 - Start preparing
 - Think strategically – broader than payments
-

Biography – Paul Anning



Paul Anning
Partner

T +44 (0) 20 7105 7446
paul.anning@osborneclarke.com

Paul Anning is head of European law-firm, Osborne Clarke's Financial Institutions Group and a specialist financial services lawyer.

With over 25 years' experience, Paul has market leading experience and expertise in the payments industry where he has guided clients through new product development, regulatory change and transformational projects, such as the creation of VocaLink, the Payments Council, Faster Payments and Paym, as well as the UK's first NFC enabled stored value mobile payment solution and a pan-European contactless mobile payment solution.

Paul is well versed in the complexities of the payments industry's network arrangements. He also has a deep knowledge of legal and regulatory developments affecting the payments industry, including SEPA, PSD, 2EMD. On PSD specifically, he has been involved since its inception in 2003.

Paul Anning is ranked as a band 1 lawyer for Payments Law in Chambers 2016, with commentary: *"Paul Anning receives widespread praise for the passion and enthusiasm with which he advises on payments regulation and is an acknowledged thought leader in the space. According to the market, he is 'pragmatic and very knowledgeable.'"*

TMT Team of the
Year
The Lawyer Awards
(UK) 2012



Law Firm of the
Year
Legal Business Awards
2015

