November 2013

When it rains, it pours - An overview of payments legislation proposals beyond PSD2

While the payments industry has been trying to grapple with the implications of the Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC (**"PSD2"**), some of the European Commission's (the **"Commission"**) other legislative proposals have gone largely unnoticed, despite their potentially significant impact on the payments market. This client briefing provides a brief overview of some of these proposals, whose interplay should be taken into account by payment service providers (**"PSPs"**) and other actors in the payment services arena.

Security in cyber-space?

The growth of the e-commerce market has brought with it a growing incidence of online fraud. Accordingly, the Commission has identified the need to address the issue of online payment security and has produced the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (the **"Cyber-security Directive"**) in an attempt to create a culture of risk management in the payments market. The Cyber-security Directive places an obligation on all EU "market operators" (which term includes credit institutions) to promote network and information security. Under its provisions, market operators have to abide by certain security requirements and to take measures to prevent and minimize the impact of incidents affecting their networks, so as to ensure service continuity. The Commission expects that through a combination of voluntary and regulatory measures, PSPs and other actors involved in the provision of payment services will undertake proper risk assessment and implement security measures that are proportional to the risks faced. Similarly, from an enforcement perspective, the Cyber-security Directive empowers competent authorities to request market operators to provide information relating to their security measures for accessing their networks, including through documenting security policies and undergoing security audits by a qualified independent body. EU Member States are also tasked with encouraging the use of standards and specifications.

Who wants a bank account?

The Commission's strong consumer focus has (once again) become evident in its Proposal for a Directive of the European Parliament and of the Council on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (the "**Bank Account Access Directive**"), which aims to promote fee transparency and account switching as well as to enhance access to bank accounts by reducing (or even eliminating) discrimination based on residency.

The Bank Account Access Directive:

- Promotes *fee transparency*, by requiring EU Member States to list the most representative services for which they charge a fee and to give access

to consumers to an independent website which offers comparative information on such fees. PSPs have to make this list available to consumers, along with a glossary of the relevant services and a "fee information" document and are under an obligation to ensure that standardized terminology, which consumers can easily understand, is used in their contractual documentation.

- Facilitates *account switching* by obliging PSPs to offer this feature and to inform consumers of this fact free of charge. The directive sets out the rights and obligations that are imposed on the transferring and receiving PSP in an account switching scenario and clarifies that any switching charges have to be in line with actual costs incurred. The receiving PSP is tasked with managing the process for the consumer and PSPs have to refund a consumer for any losses arising from the switching process due to mistakes or delays. Accordingly, the implications of the Bank Account Access Directive are quite extensive for PSPs, as they will have to ensure that they are adequately aware of all standing orders and incoming credit transfers. Moreover, PSPs will have to inform payers who make recurring transfers of the new account details, in order to achieve a seamless switching, without risk of liability.
- Seeks to achieve *non-discriminatory bank account access* for consumers legally resident in the EU, by placing an obligation on EU Member States to ensure that at least one PSP at national level offers a payment account with basic features to consumers and that consumers legally resident in the EU have the right to open and use such an account, irrespective of their place of residence and/or nationality. The proposal notes that the exercise of this right should not be made "excessively difficult or burdensome" for the consumer and sets out a list of factors that constitute acceptable grounds for the refusal of an application.

Regulating MIFs

In line with recent European Court of Justice decisions in respect of card schemes and multilateral interchange fees (**"MIFs"**), the Commission has published its Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions (the **"MIFs Regulation"**) with the aim of stipulating technical and business requirements for payment card transactions within the EU. The MIFs Regulation provides for a transitional two year period, at the end of which all cross-border and domestic credit card and debit card transactions shall be subject to an interchange fee cap (specified therein), which will also apply in respect of other agreed remuneration having equivalent object or effect. The regulation includes a strongly worded anti-circumvention provision, whereby any net compensation received by an issuing bank from a payment card scheme in relation to payment transactions or related activities will be treated as part of the interchange fee. Impacted PSPs will need to consider whether other payments unrelated to MIFs could be caught by these provisions. Restrictions in licensing agreements for issuing or acquiring payment card transactions are also prohibited.

An interesting provision in the MIFs Regulation is the article relating to separation, pursuant to which schemes and processing entities have to be independent from a legal, organizational and decision-making perspective. This provision does not apply to three party schemes and will have restructuring implications for certain businesses. In addition, territorial discrimination in processing rules operated by payment card schemes will be prohibited and processing entities will have to ensure that their systems are technically interoperable with other systems of processing entities within the EU through the use of common standards.

The MIFs Regulation also addresses certain common cards practices, and:

- Limits the application of *the honor all cards rule*, to cases where the cards have the same regulated interchange fee. Merchants deciding not to accept all cards will have to inform consumers in a clear and unequivocal manner.
- Clarifies the scope of *steering*, by prohibiting PSPs and schemes from preventing such practices.
- Stipulates that *co-badging* should operate so that the brand to be applied in each case is determined by the payer at the point of sale. Rules hindering or preventing issuers from co-badging will be prohibited and any difference in treatment of issuers or acquirers in this respect will have to be objectively justified and non-discriminatory. Payment card schemes will no longer be allowed to impose reporting requirements or obligations to pay fees on card issuing and acquiring PSPs for transactions carried out with any device on which their brand is displayed and in relation to which their scheme is not used.

Common cards practices targeted by the MIFs Regulation

- **Honour all cards rule**: obliging merchants to accept all cards within the same brand if they accept one category of cards in this brand
- **Steering**: steering consumers towards the use of payment instruments preferred by the retailer
- **Co-badging**: combining different payments brands on the same card or device
- **Unblending**: offering and charging payees separately for different categories and brands of cards

- Promotes *unblending* by ensuring that acquirers abide by it unless merchants request otherwise. Agreements between acquirers and payees have to include information on the amount of merchant service charges and interchange and scheme fees applicable with respect to each category and brand of card. With the payee's prior and explicit consent such information can be aggregated. PSPs have the option of stipulating in framework contracts that such information shall be provided or be made available at least once a month. Accordingly, PSPs will have to revisit their agreements and ensure that this information is included.

Misdirected wires

The Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds (the **"Wire Transfer Regulation"**) is aimed at enhancing the traceability of funds, in line with the Financial Action Task Force Recommendation 16. Its scope is wide - it applies to transfers occurring in any currency, which are sent or received by a PSP in the EU (except where the payer and the payee are PSPs acting on their own behalf). Accordingly, information on the payee must be included in each wire transfer, as specified therein. Where fund transfers are for an amount less than EUR 1,000 a lighter regime relating to the verification of information on the payer and the payee applies. Repeated breaches of non-inclusion of information, recordkeeping failures or a lack of risk based procedures are subject to a strong sanctions mechanism, which may translate into the loss of a PSP's authorisation and the imposition of sanctions up to 10 per cent of such PSP's turnover.

Under the proposed regulation:

- The *PSP of the payer* has to ensure that information on the payee and the payer is provided (except where both PSPs are in the EU in which case the account number of the payer suffices, provided that the payer, the payee or the intermediary PSP do not request otherwise). The accuracy of the payer's information has to be verified on the basis of information obtained from a reliable and independent source. Where a PSP regularly fails to provide information on the payer, the payee's PSP must take steps, after issuing warnings and setting deadlines, starting with rejecting or restricting payments and culminating with ending the business relationship and making any requisite reports to the AML officer.
- The *PSP of the payee* has to detect whether the information fields on the payer and the payee are appropriately filled in (and to identify if any information is missing). If the payment in question exceeds EUR 1,000, the identity of the payee has to be verified if the PSP of the payer is located outside of the EU. If the amount in question is less than EUR 1,000, the obligation to verify only applies if there is a suspicion of money laundering. The existence of missing information is considered to be a factor as to whether a transaction is "suspicious".
- An *intermediary PSP* has to ensure that the information that is present on the transfer is kept on such transfer and has to detect any missing information. Systems must be put in place enabling the PSP to determine whether to execute or reject a payment and similar steps to the ones outlined above must be taken in certain circumstances.

Conclusion

All these proposals constitute further evidence that in the past few years, the Commission has been very busy drafting a plethora of payments-related directives and regulations. Setting aside the mere volume of legislation that PSPs will need to consider and adapt to, the interplay of these legislative provisions amounts to an extra challenge that PSPs will have to tackle.

Contacts

Dermot Turing
Partner
T: +44 207006 1630
E: dermot.turing@cliffordchance.com

Simon Crown
Partner
T: +44 207006 2944
E: simon.crown@cliffordchance.com

Caroline Meinertz
Senior Associate
T: +44 20 7006 4253
E: caroline.meinertz@cliffordchance.com

Peter Chapman
Senior Associate
T: +44 207006 1896
E: peter.chapman@cliffordchance.com

Maria Troullinou
Lawyer
T: +44 20 7006 2373
E: maria.troullinou@cliffordchance.com

Laura Douglas
Lawyer
T: +44 20 7006 3907
E: laura.douglas@cliffordchance.com

J201311120044181