EU Policy Priorities for Retail Payments

Conference on 'A new era in payments?'

Lisbon, 14 May 2018

Ralf Jacob
European Commission
FISMA D.3 *Retail Financial Services and Payments*

EU regulations on payments

- *Regulations directly addressed to payments:*
  - **Legislation to lower costs**
  - **Legislation to enhance accessibility**
  - **Legislation to support innovation**
  - **Legislation to enhance security** *(money laundering, fraud, counterfeiting)*
- *A major new challenge:*
  - **Regulation on data protection**

Costs

- *Single Euro Payments Area (SEPA) significantly reduces costs for cross-border transactions in euro*
- *Interchange fee regulation (2015/751/EU) tackles competition issues in card payments market*
  - **Issuing banks and card schemes tended to apply high fees to the detriment of retailers and consumers**
  - **Caps fees for debit and credit card transactions**
  - **PSD2 prohibits surcharges for the use of such cards**
- *New proposal of 28/3/18*
  - **Charges for cross-border transactions in non-euro countries**
  - **Transparency in currency conversion**

Cheaper non-euro transactions

- *Regulation 924/2009/EU allows non-euro countries to opt in, but only Sweden did so*
  - **Commission proposes to align euro cross-border transaction costs with domestic national currency transaction costs: lower costs also for non-euro countries**
- *Currency Conversion costs to be made more transparent*
  - **Important to avoid cost shifts from transaction to currency conversion fees**
  - **Dynamic currency conversion (pay abroad in your home currency) causing detriment to consumers**
  - **European Banking Authority to develop technical standards for transparency**

Accessibility

- *Payment accounts Directive (2014/92/EU): Right to a basic bank account* allowing cash withdrawals, credit transfers, direct debits within the European Union
- *European Accessibility Act: proposal from the Commission* (COM/2015/0615, December 2015)
  - **Broad scope…**
  - **but specific requirements for banking services, including online and mobile banking and ATMs**
  - **Still negotiated between Council, EP and Commission**
- New issue on the payments agenda - ERPB group
- What role for FinTechs?

Innovation

- *FinTech has been around for some time in payments...*
- *First e-money directive adopted in September 2000 (revised by directive 2009/11/EC)*
- *Payment services directive followed in 2007, updated in 2015 to take account of new services (PIS, AIS)*
- *These directives*
  - **recognise new payment service providers and facilitate their access to the market**
  - **allow them to be licensed for EU-wide operation ('passporting')**

Regulation to enhance security

- *Crucial for public security and trust in payments*
- *PSD2 requires strong customer authentication*
- *5th anti-money laundering directive EP vote on 19/4*
  - **Customer due diligence, can be done digitally**
  - **…and will apply to virtual currencies**
  - **Strengthened Financial Intelligence Units and transparency of beneficial owners**
- *Directive on fraud and counterfeiting of non-cash means of payment Council position on 9/3*
  - **Minimum penalties, also covering virtual currencies**
  - **Better cooperation across borders**

Protection of personal data

- *Market opening to third-party payment service providers raises issues of data sharing and privacy protection*
- *General Data Protection Regulation (2016/679/EU)*
  - **Stricter rules to protect personal data, but also principle of data portability** relevant for AIS in particular
  - **Heavy fines in case of non-compliance.** Banks worried about liability in case of transmission of data to TPPs
  - **PSD2 requires minimisation of data transmission and storage**

The Second Payment Services Directive

- *Adopted in 2015, applies from 13 January 2018*
- *But only 12 Members States have fully transposed PSD2 (CZ, DK, EE, FI, FR, DE, HU, IE, IT, SK, SI, UK)*
- *Full impact also delayed due to implementing legislation:*
  - **Regulatory Technical Standards on strong customer authentication and secure communication between banks and third-party providers**
  - **Published in the Official Journal on 13 March**
  - **But applicable only after 18 months: September 2019**

PSD2 as innovation enabler

- *Better consumer protection to strengthen trust in electronic payments*
  - **Ban on surcharges for card payments**
  - **Reduced maximum loss in case of fraud** (from €150 to €50)
  - **15-day deadline for responses to complaints and out-of-court redress**
  - **Strong customer authentication to reduce fraud**
- *Recognition of new 'third-party' payment service providers*
  - **Payment initiation services**
  - **Account information services**

Strong Customer Authentication

- *High level of protection by using at least two independent elements from the categories below:*
  - **Knowledge** (of a password or PIN)
  - **Possession** (e.g. card, code generating device)
  - **Inherence** (personal characteristics, e.g. fingerprint, voice)
- *Numerous exemptions*
  - **Low value and contactless payments, transport / parking fees**
  - **Trusted beneficiaries and recurring transactions**
  - **Transaction risk analysis, if it keeps fraud levels low**
- *Monitoring obligation when exemptions are used*
- *Review clause for the fraud rate thresholds*

Secure communication (1)

- *Bank customers must not be prevented from using new services of Third-Party Providers (TPPs)*
  - **Payment initiation services:** Provider triggers a credit transfer from a customer’s bank account to a payee; replaces card payments
  - **Account information services:** Providers get information from different accounts and offer personal finance monitoring and management services – other uses may emerge
- *TPPs often use ‘screen scraping’: accessing online banking interface with bank customer’s credentials*
  - **Regarded as unsafe**
  - **Requires major investment in software by TPPs**

Secure communication (2)

- *PSD2 requires banks to provide account information to TPPs*
- *Communication must allow identification of TPPs and exchange of security certificates*
- *Only information needed for a transaction to be obtained*
- *Two options for interfaces*
  - **Adapt the customer online banking interface**
  - **Create a dedicated interface which would then be mandatory for TPPs** – but lack of trust among TPPs
- *Dedicated interfaces best for rapid development of the market for new payment services*

Towards EU-wide open banking

- *PSD2 does not mandate a standard API, unlike UK CMA*
- *RTS empowers banks to mandate it:*
  - **TPPs must use banks' APIs, no more 'screen scraping'…**
  - **…provided the API is of good quality; otherwise: adapted online banking interfaces as a fall-back for TPPs**
- *RTS provides incentives for standardization:*
  - **Banks want to avoid costs of fall-back…**
  - **…and can be exempted by NCA if they provide an API that is accepted by all market players**
  - **Use of standardized APIs increases chances of exemption**
- *EU evaluation group established by market players to review API standards*

A difficult transition to open banking

- *PSD2 applicable from 13/1/2018, but key requirements for secure communication only in force around September 2019*
- *Grandfathering: TPPs that existed before 12/1/2016 can offer the same activities in same markets as before*
- *New and existing TPPs licensed under PSD2 allowed to access accounts using screen scraping in all MS except those where it had been illegal before 12/1/2016*
- *But MS must ensure that banks do not abuse their own non-compliance with security standards to block or obstruct the use of payment initiation and account information services (Article 115(6), PSD2)*
- *EBA opinion on the transition: comply with RTS as soon as possible*

A new era in payments?

Drivers of change:

- *Regulation: what can third parties do with account access and information – PSD2 and RTS implementation, complying with data protection rules*
- *New infrastructure and technology: instant payments, mobile payments*
- *Innovation and competition: how will market players respond?*

The impact of regulation

- *Right for consumers to use new services: payment initiation and account information*
- *Incentive to develop standardized APIs: lower barriers to market entry*
- *Strict data protection rules under PSD2 and GDPR may limit business models relying on exploiting personal data:*

  Article 67(2)(f), PSD2: AISP shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules

The impact of new infrastructure

- *Instant payments already available in a number of non-euro Member States*
- *Eurozone catching up:*
  - **SEPA instant credit transfer scheme (SCT inst)**
  - **TARGET Instant Payment Settlement (TIPS)**
- *First application could be for mobile peer-to-peer payments*
- *Major impact when used by consumers for purchases*
- *Further enhances the possibilities of simple payment accounts; no need for credit cards or guarantees to merchants*

Who will be the dominant providers of payment services?

- *Banks competing with attractive apps and offering overdrafts to replace credit cards*
- *FinTechs providing the interface to banks which will 'mass-produce' account services with little direct contact to customers*
- *“Big Tech” players adding payment initiation and account information services to their mobile apps*
- *Mobile phone operators*
- *National card schemes developing payment solutions for a country's banks*
- *Global card or e-wallet schemes leveraging their brands and global acceptance with merchants*

Key question: how to make money with payments

- *Levying charges on merchants? Instant payments could allow cheap alternatives*
- *Account fees? Low acceptance by consumers*
- *Free payment accounts to attract customers for other services?*
- *Fees for payment instruments with premium features? (insurance, chargeback rights...)*
- *Personal data for free payment services?*