The regulatory challenges posed by electronic financial and payment services

This document was drafted by Eurofi with input from its members. It does not engage in any way the Italian EU Council Presidency nor the Italian Financial Authorities.

1. Digital innovation raises new challenges for financial institutions

Technological developments continue to impact the EU financial institutions. Controlling costs or mitigating risks systematically involve the processing of data and analytics. Delivering to increasingly differentiated customers the same level of service through the channels they select, whether mobile, tablet, PC or branch also require major processing and support investments from financial institutions. Some customer segments are in addition prone to adopt innovative products and services – financial or non-financial – that fit their changing needs. In particular technological innovation creates new commercial contexts which demand innovative answers to traditional needs (payments, financing, security, etc.). Finally big data and cloud computing are becoming important tools for better understanding customer needs and providing them with an improved experience.

These challenges imply far-reaching changes for banks, as their systems are complex, with reduced connectivity among different applications, which results in rigid and unattractive services. In addition “cooperative innovation” models are also needed, such as when a bank opens its technological platform to outside developers in order to create services. Employees, clients, telcos, etc. among the various possible stakeholders must be involved at every step. Indeed the proportion of consumer interaction taking place through branches is constantly declining and many financial services will result from or involve partners of widely varied natures (apps developers through the application of programming interfaces, specific commercial digital businesses, etc.).

2. Regulators are also challenged by innovation in digital financial services

Such issues regarding innovation in saving product distribution or financing offers that are being tackled through specific regulations (Mifid, Shadow banking, etc.).

In the retail payment area the EU Commission is trying to tackle some of the issues resulting from technological and market developments and from the emergence of new players. There, new entrants are exempt from the legacies of banks such as obsolete systems and costly distribution networks. PayPal, Square, iZettle, SumUp, or Dwolla, which have specific added value and business models in the payment area are expanding. In addition certain leading firms in the digital world such as Google, Facebook, Amazon, etc. - are also developing payment services.

Moreover, many new payment operators are competing in the market after the implementation of the “Payment Service Directive 1”: the European Commission counts more than 600 Authorized Payment Institutions and 2100 “Small” Payment Institutions in the European market.

Finally this raises a regulatory challenge. Regulators need to ensure security, privacy, consumer protection and systemic stability. At the same time, they should leave space for innovation but maintain fair competition. This must be completed in a digital world that is largely unmapped and gets bigger, faster and more complex by the minute.

One of the challenges can be summarised in the following manner. Innovative products possibly create a sensitive situation by which a Third Party Provider (TPP) embedded in the innovative product, obtains the sensitive private and secret credentials of a consumer and uses them to impersonate the consumer, enter the bank account and initiates a payment order as if it were the consumer.

Furthermore almost every account holder in the EU possesses a debit payment card and 40% also own a credit card. 34% of EU citizens already shop on the Internet and more than 50% possess a smartphone, which allows them to access the world of mobile payments. At the same time certain economy sectors make most of their sales on the Internet. However, the EU market for cards, internet and mobile payments remains fragmented and faces important challenges that hinder its further development and slow down the EU growth potential.

Regulators need to prepare for the increasing digitalization of commerce and payments. The rising digital economy needs adequate online identification procedures, which are applicable to account-holding as well as transactional payment operators such as money transfer operators. There is a need for harmonized electronic identification and authorization tools to better support the growing field of digital non-face to face transactions and a need to become more tech-savvy in applying modern technologies to AML-KYC procedures.

Finally, beside Data Protection rules, or potentially also the new Security Requirements and despite the much needed harmonization which the PSD2 has brought to one part of the European legal framework, other relevant areas do not yet benefit from a Single Market approach: in particular the Anti-Money Laundering rules.

In a rapidly changing market, it is important to target guiding principles when refining the future regulatory regime for payments. These principles need to include: i) legal certainty and regulatory consistency; ii) proportionality and technological neutrality; iii) the fostering of financial inclusion, and, importantly iv) an effective promotion of the Single Market for retail payments.
3. As an answer to such challenges the PSD2 is expected to clarify the rights and duties, of both Account-holding Payment Service Providers and Third Party Providers

The PSD 2 seeks to respond to the changes in the way Europeans shop and pay. In that context the objective of the revision of the payment service directive (PSD 2) proposed by the European Commission is in particular to help to develop further an E.U.-wide internal market for electronic payments in particular by facilitating the access to payment accounts by third party providers.

The PSD 2 is expected in particular to clarify the distribution of rights and duties, between Account-holding Payment Service Providers (APSP) and TPPs. Also the minimum-security standards required from TPPs to access an account, need to be better defined. Their respective responsibilities in the case of a possible defective execution and conflicts need also to be clarified.

Banks in that respect, question the existence of business models based on the transfer by the consumers of their personal credentials. This demand a level playing field imposing the same safekeeping, security, privacy and transparency obligations to TTP as those imposed on APSPs, and claim a fair distribution of the responsibility between TTPs and APSPs, and a fair cost sharing whenever a TTP generates activity within the account-holding APSPs.

In addition the banks question the focus of the PSD2 on TPPs, which is specific to the E.U., as the current situation has not impeded a swift and continuous, double-digit growth of the e-commerce market. Finally the banks consider that no “market failure” has been evidenced, which would justify legislative intervention and the related compliance costs.

More generally as in the area of prudential requirements, payment services also demand a single and consistent rulebook as well as consistent supervision across the E.U.

In such a context, the compromise reached by the Greek presidency has introduced a definition of the service provided by TPP, identified critical and sensitive payment data, and introduced various safeguards. It further defined the role of the EBA regarding a possible need for settling disagreements between competent authorities of different member states, and the powers of host member states regarding the compliance of business activities with national laws, mandatory information to be made available to payers by TPPs, the obligations of the TPP regarding the accessibility of information related to the payers’ account. Lastly the compromise introduced the prohibition of the request from the payer to provide re usable credentials. It also adjusted TPP liabilities regarding in particular unauthorised payment transactions.

4. The PSD2 is discussed in the context of increasing fraud

These discussions are held against a background of increasing fraud in particular in card transactions. In that respect although only 2% of all card transactions were acquired from outside SEPA, they accounted for 25% of all fraud in 2013. In addition with €794 million in fraud losses in 2012, card-not-present (CNP) payment fraud, i.e. fraud on payments via the internet, post or telephone, was not only the largest category in absolute value, but also the one with the highest growth (up 21.2% from 2011).

Indeed cyber attackers are increasingly combining “malware-based” Web injection with server-hosted scripts in order to piggyback on active online banking sessions and initiate fraudulent transfers in real time, McAfee and Guardian Analytics researchers said. By extrapolating the data gathered from the European attacks, security researchers estimate that cybercriminals attempted to steal between $75 million and $2.5 billion using fraud automation techniques.

These attackers after reading account balances, transfer predefined sums to money mules -- intermediaries -- the selection of which is also made automatically by querying a constantly updated database of money mule accounts. The SEPA provides an attractive target in that respect. For example in the attacks McAfee identified, fraudsters initiated SEPA credit transfers through an automated transfer system (ATS), which sends a withdrawal request to the victim's account and credits a mule account. Such attacks usually target high-balance accounts owned by businesses or high net-worth individuals.

Automated fraud also allows cybercriminals to bypass two-factor authorization systems implemented by banks for security purposes. Malwares capture customer’s keystrokes including their bank login credentials, and sends the data to the criminal. Consequently compromising one site, criminals may gain access to credentials to many others by exploiting the re-use of a password as managing user names and passwords for a multitude of banking gaming and social media sites can be overwhelming.

Similar to a “phishing” email scheme, in the context of the explosion in smart phone usage, by “smishing” criminals have found a new way to gather the data they need to commit fraud. Finally bank insiders are also involved. Most bank employees have access to customer data; therefore, cybercriminals often attempt to coerce, bribe, blackmail or trick them into disclosing such information.

1 Third report on card fraud – ECB - February 2014.
2 Cybercriminals increasingly use online banking fraud automation technique Computerworld 26 June 2012.
In such a context banks deploy many defences including Geo-location based on the IP address associated with the customer location, Device recognition and Transaction monitoring, by which software reviews customer’s activity for anomalies or red flags, which are indicative of possible fraud. Banks also control Navigation Cross channel: they monitor and analyze user behaviour across a range of payment and channels to determine if there is a correlation between behaviour and the probability of fraud.

5. Improving competition conditions in the E.U. in the card payment services

- The Commission considers that a regulation is necessary to further integrate the EU card market and improve competition.

The Commission considers that cardholders are encouraged by banks to use cards that generate higher fees, as card companies compete primarily to attract issuing banks by offering higher interchange fees. In such a context new and innovative providers of mobile or online payment services cannot enter the market and (low fee) domestic operators cannot expand throughout the E.U. as banks expect the same (high) revenues.

National and E.U. competition authorities and regulators have been looking at interchange fees for some time. In addition certain card scheme rules preventing merchants from steering consumers in the choice of a payment instrument (rebate, surcharging, refusal of a payment instrument) have also been covered.

However the European card market remains fragmented and interchange fees vary widely across the E.U. Moreover the Commission considers that competition enforcement due to its nature, cannot address existing imbalances and obstacles for a level playing field to emerge in a comprehensive and timely way.

The Commission in this context considers that a regulation is necessary, which is expected in addition to guarantee the legal certainty of a card payment business case.

In particular the E.U. Commission proposes in its draft regulation, 0.2% and 0.3% caps on interchange fees, levels that were proposed by certain schemes (Visa Europe, MasterCard, Groupement des Cartes Bancaires) in competition proceedings. These levels stem also from data from the central banks of Belgium, the Netherlands and Sweden on the cost of payment instruments, these data were computed to estimate the fee at which a merchant would be indifferent between being paid by card or in cash. This is also intended to provide sufficient legal certainty for card scheme business cases.

Consistently, "three-party" card payment-schemes using issuers - which represent according to the Commission 9% of Amex cards and all of Diner's - would also be covered by the caps on interchange fees.

- The concrete policy options are not obvious

However the concrete policy options are not obvious. Indeed the most important function of interchange fees is to balance the demand of cardholders and merchants for the cards of the scheme so as to maximize the value of accepting cards to both groups of users.

Actually if interchange fees are too low, acquiring banks will find it easy to sign merchants up to accept payment cards, but issuing banks will have less incentive to issue the kinds of cards cardholders want at the price they are willing to pay. An imbalance in the long run, benefits neither cardholders nor merchants. Conversely, if interchange fees are too high, issuing banks will issue many cards, but merchants will be reluctant to accept them and will favour cash instead, despite the considerable costs and risks involved in handling it.

In particular interchange fees do encourage issuing banks to undertake the considerable investments necessary to market safe payment card products to their customers. Issuing banks have considerable outlays in offering card payment services to their customers, including those for card production and distribution. They finance a possibly interest-free period, fight against fraud and face credit losses and also contribute to ongoing innovation.

More generally Banks stress the fact that interchanges are remuneration for services.

Finally the risks associated with regulating these interchange fees, whether this involves capping or prohibiting them, will entail higher costs for card usage by consumers, more cash transactions that gives a helping hand to tax dodgers, fraudsters, money launderers and other criminals, less payments innovation, security and efficiency.

Many banks oppose the situation observed in Australia, where interchange fees were capped and where there has been a slowdown in the growth of card payments. Moreover, they say that there the capping of interchange fees and the resulting cost saving for merchants, did not benefit consumers. Instead, it resulted in their paying more to use cards with no detectable reduction in the prices of goods and services.

In addition banks fear that regulating inappropriately interchange fees may inadequately favour three party payment schemes, which is detrimental to competition.
More generally they stress that the legitimacy of any single regulation requires proof in each country within the E.U. that card schemes are in a dominant position.

On the other hand, smaller networks claim not being included in the scope of any IF regulation. They consider indeed that they do not have the characteristics of dominance or collective practices, which are addressed by such regulatory provisions. On the contrary they protest that such measures would dramatically undermine their economic viability as well as the ability of smaller networks to act as a counterweight to dominant schemes.

Similarly digital wallets warn against any attempt to assimilate them to card schemes with respect to such caps, as they do not engage in card-based transactions and are users of card schemes and pay interchange fees to the four-party scheme acquiring banks.

In addition certain small networks consider that the proposed rules do not acknowledge that in some circumstances territorial restrictions are the appropriate counterpart of the investment made by a licensee. Indeed they consider that this plays a critical role in promoting the competition of networks whenever their share of the market is small in a given country. Similarly small networks stress that “steering requirements” with merchants, are part of the commercial flexibility that they need.