INNOVATE. COLLABORATE. DEPLOY.

The EBF vision for banking in the Digital Single Market

EBF
European Banking Federation

Brussels, 14 November 2016

Introduction

Banks can play a decisive role in the development of the European digital single market. On the one hand, banks are the main source of finance to the European economy that is undergoing a process of capital-intensive digitalisation. On the other hand, banks - guided by customer demand - are heavily investing in technology and partnering with technology startups to improve customer offerings and to transform their business models.

In recognition of the above, Commissioner Oettinger has set up a Roundtable on Banking in the Digital Age with a number of bank CEOs, representatives of the sector and the EBF. The Roundtable has laid down the foundation for a collaborative approach between the Commission and the industry in the form of a structured dialogue with DG CONNECT and other directorates of the European Commission (foremost with DG FISMA and DG JUST). The participation of Vice-President Dombrovskis in the Roundtable is particularly welcomed.

The objective of the Roundtable is to identify what should be done at EU level to help enhance banks' competitiveness and their ability to leverage digitalisation more effectively to serve citizens and firms, as well as to identify how banks can continue to support the European economy, in particular by investing in innovation, and what should be done at other levels, including by banks themselves.

1. Consumer demand as the key driver of banks' digital transformation

Consumers around the world are quickly becoming digital. They want to manage their money more proactively, to simplify and streamline the management of their financial portfolio, and be able to derive tangible benefits from their service providers. As a result, consumers expect a new kind of service proposition from banks, fitting to the digital age.

In response, banks - and other providers - are assessing, developing and using innovative and technological capabilities (such as open APIs, blockchain, robo-advice and machine learning) to develop new delivery channels as well as to enhance services and products that deepen the relationship with their customers. Those digitally enabled services allow banks to leverage their core capabilities in areas such as product expertise, human capital and customer insight. In short, the use of new technologies helps banks maximise customer experience.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

2. Banks as strategic partners for the Digital Single Market

Banks are accelerating the digital transformation of Europe in three main ways:

1. As direct investors in new technology and more broadly in the digital ecosystem - banks invest $700 billion annually on IT innovation – a fifth of global total expenditure. These investments go far beyond maintenance and development of in-house solutions, but also includes investments in Fintech startup companies, not only financially but also as knowledge sharing and an increased reach. Banks have launched incubation and acceleration initiatives, as well as other investment vehicles that harness, foster and scale-up innovation. Networks of startups are emerging around an ecosystem anchored by individual banks. This is leading to vital growth in the technology sector, to job creation and accelerated innovation.
2. As financiers of the European economy (80%), including its digital infrastructure. European banks are making financing available to support the growth of European companies, so that they are able to compete with foreign firms.
3. As enablers of the public sector's digitalisation: the public sector and the banking sector have a large degree of interdependence when it comes to digitalising each sector's respective processes. In some Member States, the use of digital public services occurs on the back of banks' security systems. Conversely, banks are, for example, highly dependent on digital land registry services for developing fully-automated loan application services. Although the status of these kinds of interaction vary amongst Member States, there can be no doubt that an increase in this form of cooperation would be a helpful development for continued digitalisation of the economy, and for a Digital Single Market in financial services to unfold.

3. Banks' partners and competitors in their digital transformation - we are all innovators

The combination of customers' evolving preferences and technological advances allows for banking in a very different way. It also creates space for new entrants to serve the market. The European banking industry supports the Commission's policy to promote more competition, including in financial services. As was rightly pointed out by one of the CEOs at the first meeting of the Roundtable, we are likely to see increasing cooperation and partnership in the banking sector among incumbent banks and new Fintech startups providing innovative products and services to the market. Indeed, the arrival of Fintech startups and the establishment of digital platforms has spurred innovation, accelerated the transformation of banks and opened a door to new win-win collaborations. Thus the ongoing digital transformation of banks must continue to be supported by the Commission as a means of increasing competition in the sector.

While there are still good reasons for banks to rely on internal IT departments, there is considerable potential to create value — for themselves and the economy at large — by nurturing an ecosystem of startups and technology innovators that can assist banks in developing shared platforms increasing resilience and cost effectiveness of banking and payment systems. Banks have a lot to offer to Fintech startups, in particular, specific financial expertise (risk assessment, evaluation and management), scalability owing to their large customer base, as well as many years of experience in providing clients with regulatory-driven high levels of operational security, not to speak of financing needs. The strengths and weaknesses of both banks and Fintech startups mean that both will often do better by cooperating rather than by competing (as recently assessed in the UK, 80% of the Fintech startups are aimed at supporting incumbent banks). However, deepening cooperation with Fintech startups is constrained by banking regulation as described further on (see below in this document).

Strong competition between banks and non-banks is also taking place to the benefit of customers. This competition is healthy for the market and should be encouraged by enabling both incumbents and new players to deploy their digital strategies within the boundaries of a regulatory framework that equally supports both all market participants.

4. The impact of regulation & supervision: enabling the digital transformation by all and for all

Stringent prudential, security, investor and consumer protection regulation are an inherent part of the regulatory framework in which banks have to operate and which has been reinforced in recent years. New entrants are less burdened by regulatory requirements and they tend to choose the optimum legal structure to avoid the heavy regulatory burden of the financial sector. Similarly, they are not subject to the same levels of scrutiny from supervisors and authorities. The implications of this for policy objectives concerning consumer/investor protection, fraud and financial crime, and financial stability must therefore be considered.

Finding a proper balance, and future-proofing it, will be one of the main (and on-going) challenges for policymakers, regulators and supervisors for the years ahead: how to encourage the development of financial technology and to bring dynamism and competition into the financial sector both for incumbents and new entrants without leaving the financial sector open to new risks or significant failures and thereby endangering financial stability, with possible loss of public confidence, or creating an uneven regulatory framework. Customers and investors' trust will be gained if they are confident that the same level of protection is available no matter which entity – banks or non-banks alike – is providing the financial services.

From a supplier's perspective, the concern is that a loss of trust by consumers in one area of the industry, whether that be a Fintech startup or a large incumbent, hurts the sector as a whole. With equal rights must come equal responsibilities. Cybersecurity is a good example of this principle. A failure by any single market participants hurts the reputation and damages trusts in the industry as a whole. Policy makers should consider the importance of ensuring that a high regulatory standard is applied and supervised across all market participants. In the nutshell, the concept of "same services, same rules, same supervision".

Technology (and digital platforms) neutrality and cooperation are also important concepts in this respect, as otherwise banks will face competitive disadvantages from certain competitors that control digital platforms on which banks and many other businesses also fully depend on offering their digital services.

The Digital Single Market is an opportunity for all operators willing to embrace the digital transformation: authorities, banks, Fintech startups, corporates and consumers. The achievement of their respective digital ambitions calls for a regulatory framework that takes into account three important considerations:

1. Allow for competition to unfold: a number of adjustments to existing legislation / regulatory frameworks and right-sizing of regulatory requirements need urgent attention for competition and a Digital Single Market for financial services to take off, and must be addressed in the short term (see point V).
2. Put Digital first: a thorough fitness check by the EU of the existing complex regulatory framework is necessary to ensure it is fit for purpose to support banking in the digital age. To be clear we see no need to create new regulation for the digital era but consider it important to make a thorough and comprehensive review of existing legislation to ensure the current framework is up to date, future-proof and does not impede innovation and competitiveness in the Digital Single Market for financial services. Furthermore, regulation must not unduly constrain banks or Fintech startups from providing an effective response to the challenges posed by digitalisation.
3. Promote innovation and avoid unintended disincentives: regulation can also be observed as a disincentive to experimentation. Undertaking regulated activities in various Member States usually requires explicit permission from the regulator and approval of the way in which the firm in question goes about its business. A risk-averse regulator may not be willing to grant permission to unfamiliar or unproven business models. Unregulated entities may, however, find it easier to undertake new business without having to comply directly with the regulator's tests. Similarly, digital services can easily cross borders, and varying risk appetite among regulators and overseers may hamper the cross-border provision of services and unintendedly lead to market distortion.

5. Key issues to be addressed rapidly

At the first meeting of the roundtable, participants identified areas where actions could be taken by the Commission in the short to middle term:

- E-ID and digital onboarding
- Regulatory/Prudential/Accounting rules applicable to the banking sector
- Data
- Cloud
- Cybersecurity
- Platforms
- Payments

In addition, the questions of improving the level of digital skills in Europe and the financing of the Digital ecosystems (notably digital infrastructure) were underlined.

The different blocks have been a subject of many discussions within the EBF's dedicated group of experts. The experts have engaged regularly with the relevant Commission services. Furthermore, meetings have been organised by the Commission (DG CONNECT with the participation of other relevant DGs) with the bank Sherpas involved in the roundtable, since 5 April 2016. On each occasion, these meetings enabled participants to take stock of the progress achieved in each workstream.

ISSUE 1:
E-IDENTIFICATION AND DIGITAL ONBOARDING

Problems/issues

1. Digital onboarding & AMLD

Consumers are becoming more digitally and globally-oriented, which calls for simple and user-friendly digital onboarding solutions by banks and financial services' providers including distant digital onboarding. The eIDAS Regulation clearly presents e-identification and e-signature as a new opportunity to facilitate the establishment of non-face-to-face business relationships. Currently, however, there is inconsistency between eIDAS, which promotes e-identification to access online products and services and to carry out online transactions safely, and the 4th AML Directive which still favours face-to-face customer due diligence and considers non-face-to-face relationship as a "high risk", requiring Enhanced Due Diligence.

We welcome the possibility to identify customers and to verify their identity on the basis of electronic identification means. The reference to Regulation (EU) 910/2014 (e-IDAS) in the EU proposal amending the 4th AML Directive appears to be a step in the right direction. Even though the eIDAS regulation can bring coherent framework for e-identification services in the long term, the recognition of notified electronic identification schemes under eIDAS will only be mandatory as of September 2018 (notification and recognition of notified eID means by Member States started on a voluntary basis in September 2015). This situation may bring unacceptable delay for the customer onboarding perspective. Currently there are widely used, sufficiently secure and operable services which are not and might not be notified as eIDAS. A truly Digital Agenda must keep the door open to further progress. In the context of the revision of the 4th AMLD it should be guaranteed that existing and future processes and services outside the scope of eIDAS can be accepted under the revised AMLD at least when they are approved by the competent authority.

Consequently, it is important to take an even bigger step forward on the Digital Agenda by including in the 4th AML Directive any other remote identification processes recognised and approved by the competent authority.

With respect to **the need to ensure a consistency in the implementation of the 4th AMLD across Member States**, it is paramount to generate an environment in which national authorities and the financial sector can collaborate in an efficient way at European level in order to share best practices. This will enhance the security for the whole digital market, and at the same time help guarantee a level playing field for financial entities who wish to operate across European Markets, by establishing best practice standards for the identification of customers new to banks. For example, in relation to electronic identities, some EU Member States allow the use of non-face-to-face identification for customers by means of videoconference, while others do not. As a result, financial institutions in these Member States can initiate distance banking relationships (including cross-border), whereas other financial institutions are prevented from doing so in their own jurisdictions, due to face-to-face identification still being required.

2. eIDAS Interoperability

In addition, it is important to recall that even if eIDAS Regulation creates an interoperability framework for the national eID systems to be recognised by public bodies across the EU, it remains up to Member States to define the terms of access to the online authentication of government eIDs by the private sector. It leads to insufficient mutual recognition of eIDs issued in other Member States and **a lack of cross-border interoperability of national eIDs.**

3. eIDAS attribute-set

eIDAS plays an important role in supporting economic growth in the EU by leveraging ease and interoperability of digital cross-border services. For this reason, it is important that eIDAS finds a fast and widespread take-up across industries throughout the EU. A good push for leveraging eIDAS take-up is to facilitate smooth adoption of eIDAS by the financial sector, which has an enormous digital footprint to make use of. To facilitate the adoption of eIDAS by the financial sector, **it is important that the identity attribute-set coming with eIDAS is in synch with the identity information-set banks need when onboarding a customer, according to the AML**. **The more complete the eIDAS attribute-set, the more attractive the eIDAS solution**, as this removes a sizeable impediment to collecting and verifying extra data-attributes and lessens significantly the effort required by banks. In order to promote the adoption of eIDAS by banks, enlarging the basic eIDAS identity attribute-set to include additional attributes, requisite for client identification in the Financial Sector would be of great value (for example making the customer address mandatory and allowing banks to validate ID documents digitally).

Reference Directive(s) and/or Regulation(s): 4th Anti-Money Laundering Directive (Directive 2015/849/EU); Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal mark

Proposed solutions

- **Recommendation 1:**

  Amendment to Article 13 of the proposal amending the 4th AML Directive and other related articles:

  "Customer due diligence measures shall comprise identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source; including, where available, electronic identification means, as set out in Regulation (EU) No 910/2014 or any other remote identification processes recognised and approved by the competent authority."

- **Recommendation 2 :**

  To promote cross-border interoperability in the banking sector and ensure a level playing field across Member States (and possibly beyond in EEA countries and Switzerland), we would recommend leveraging the work carried out under the Connecting Europe Facility Programme, by reusing the eID Digital Service Infrastructure (DSI) and setting up a

financial sector specific DSI which could in particular look into the needs of the banking sector with regard to the digital onboarding.

This financial sector specific DSI could investigate the needs of the sector with regard to digital onboarding, with the objective of establishing good practices in countering money laundering, and the elements/attributes which are required to potentially ensure the portability of the Know Your Customer (KYC). The work carried out could then possibly be used by national authorities as a benchmark in their dealings, with the aim of promoting cross-border activity in the financial sector and ensuring a common level playing field across Member States.

ISSUE 2:
PRUDENTIAL REGULATION

Problems/issues

Banks willing to transform to digital have to invest intensively in two critical areas: software and digital talent. However, prudential regulation restricts both of these areas in different ways. As this regulation only affects banks, it also creates a weaker competitive position for them.

Investments in software are restricted for banks in general, but especially in the case of entities based in the EU, where the accounting treatment of software as an intangible asset causes it to be fully deducted from the Core Equity Tier 1 (CET1) when calculating the capital requirements. This is perceived as a significant disincentive for investments in innovation and a major factor of unfair competition.

Software has become a core asset for the banks' business models around the world. However, there is evidence of different regulatory treatment of software in some jurisdictions, including the United States where capitalized computer software can be recorded as "other assets" and subject to regular risk rating and not deducted. Consequently, this removes any artificial hurdle to banks investing in digital, creating value for the economy as a whole and leading worldwide innovation in the area.

The regulatory approach to software of the European regulators already acknowledges, to a certain extent, the fact that software has the capacity to generate value when it comes to the treatment of software for solvency purposes for the insurance industry. Under the solvency framework for the European insurance industry, intangible assets[1] can be recognized for capital purposes as long as it can be demonstrated that there is a value for the same or similar assets. We believe the investments in software should carry the same economic and financial rationale, regardless of the industry. Whilst this may not be sufficient, it sets the basis for the solution to the issue in the banking field. Evidence clearly indicates that software has value even in the case of liquidation of a bank as proved in a factual analysis of Price Waterhouse Coopers (at disposal).

Furthermore, the European Commission issued decisions on equivalence of the regulatory regimes of third countries to those applied in the EU. Capital regimes of third countries that do not require capital deduction for software have not been considered as an element of relevant discrepancy or inconsistency for the European Commission, neither for the Basel Committee under its Regulatory Consistency Assessment Programme. A change to the Capital Requirements Regulation (CRR[2]) is therefore justified.

Engaging and retaining digital talent in banks is also affected by prudential regulation in Europe. In order to reduce the incentives for banking employees to take excessive risks, the rules constrain the variable remuneration that an employee can receive (not to mention other rules such as the deferral of payment or part of the payment in instrument of the financial institutions etc.). This limit affects digital specialists who do not perform risk taking (including operational risk) activities but are critical for the digital transformation.

[1] Under IFRS, software has to be accounted for as intangible asset unless it is an integral part of the related hardware

[2] Regulation (EU) No 575/2013pdf on prudential requirements for credit institutions and investment firms (CRR)

Without challenging the remuneration framework itself, it matches very badly with a digital environment where innovators tend to be remunerated with equity participation that encourages entrepreneurship. Consequently, it is extremely difficult to attract and retain scarce digital talent when banks cannot offer packages that compete with their digital peers.

The strengths and weaknesses of both banks and Fintech startups mean that both will often do better by cooperating rather than by competing. As a result, many banks are willing to support or cooperate actively with Fintech startups. Deepening collaboration with Fintech startups is however restricted by banking regulation, especially if the bank decided to acquire a significant stake in the company. The valuation of a startup acquisition is lower for the bank than for any other kind of competing acquirer, from a bank's point of view (the latter would need to raise more capital for the acquisition in order to mitigate the impact of the deduction in software and increase the fixed term of the compensation package for the key digital innovators in the Fintech startups). From the Fintech startup's point of view, this reduces the range of exit strategy options for their investors, as there would be less appetite for acquisition from the side of one of their more natural acquirers. These are in our opinion, unintended effects of the prudential regulation that should be addressed.

Finally, we would like to point out that draft proposals issued by the Basel Committee to complete the Basel III framework suggests changes that could increase the Risk Weighted Assets for specialized lending, including for infrastructure financing, mainly due to the potential removal of internal rating-based models. This would be contrary to the Juncker's Investment Plan for Europe and has potential to limit long-term investment in the EU (IT) infrastructure. Considering that a default rate of project finance is in general low[3], we would like to suggest that the EU recognizes this reality by assigning long-term investment in growth promoting (IT) infrastructure lower capital charges. The precedent for this can be found in Article 501 of the CRR which introduces the so-called SME supporting factor. In this respect we would recall that since its introduction, the SME Supporting Factor has had a crucial role in allowing banks to reallocate resources to the benefit of the real economy and we would recommend a similar measure to be considered for project financing. Moreover, the upcoming revision of the CRR should consider an appropriate calibration of the Net Stable Funding Ratio requirement (NSFR) so as not to impose additional constraints on the long-term investment in growth promoting (IT) infrastructure.

Reference Directive(s) and/or Regulation(s): Capital Requirements Regulation (CRR); Commission Delegated Regulation (EU) 604/2014 on identification of staff.

Proposed solutions

- **Recommendation 1:**

Amendment to the CRR: "Article 4 Definitions: (115) "intangible assets" has the same meaning as under the applicable accounting framework and includes goodwill, **with the exception of software for the purpose of Article 36**".

- **Recommendation 2:**

Amendment to Commission Delegated Regulation (EU) No 604/2014: "**The approval requirements set out in Paragraph 5 shall not apply when the staff member meets either of the following conditions:**

[3] https://www.moodys.com/research/Moodys-Project-finance-remains-resilient-class-of-specialised-corporate-lending--PR_345857

a. carries out professional activities that are not exclusive to companies under the subjective scope of CRD IV in a function or unit related to digital transformation of the institution or to the development of digital businesses;

b. was already employed in a digital firm acquired by the institution and his or her remuneration scheme is set before or at the time of the acquisition and is conditional on continued employment in the company.

An institution applying this paragraph shall keep a record of the professional activities carried out by the staff member and a reasoned explanation as to why conditions (a) or (b) are met. This record should be readily available upon the request of the competent authority responsible for its prudential supervision".

- **Recommendation 3:**

Address the obstacles posed by draft proposals on the revision of the Standardized Approach for credit risk (Basel IV) that aim at substantially increasing the Risk Weighted Assets for specialized lending, including for infrastructure financing.

- **Recommendation 4:**

The EBF will organise a workshop in 2017 on "Mobilising private finance for the digitalisation of the European economy", jointly with the Insurance sector, giving the Solvency II ramifications.

ISSUE 3:
CLOUD

Problems/issues

Technological progress and globalisation have led to significant changes in methods of data collection, access and use. Over recent years, this has contributed to an observed increase in banks' interest in cloud computing as a means to support the sustainable digitalisation of the banking sector through potentially:

- enabling innovation;
- introducing new solutions to improve IT security and reduce IT risks;
- enabling cost efficiencies; and
- facilitating more competition in the sector.

It is important to highlight that cloud computing represents a major source of growth for European Union (EU) economies and that such benefits are optimised when they can be leveraged consistently and across borders, particularly where global banking businesses are seeking to provide services to global customers.

While technology in banking has adapted to business requirements within the legal and regulatory constraints applicable at local, national and regional level, banks have nevertheless been seen to be slower in migrating services to the cloud when compared to other industries. We observe that the legal and regulatory constraints and the higher compliance risk derived from the use, management and storage of customer information constrain the adoption of cloud service models by a strictly (and comprehensively) regulated banking industry. These constraints also create significant frictions in ensuring that regulatory compliance is achieved in contractual negotiations between banks and cloud service providers (CSPs).

Another key factor slowing down cloud adoption in Europe is the lack of harmonisation in regulatory approaches across different jurisdictions. The variation in approach to cloud computing in financial services by various national regulators creates inefficiencies, particularly for banks operating with a global presence and global customers. The uncertainty created by the variation in approach reduces the appeal of the EU as a place to do business. This is not unique to the incumbent banking industry. New FinTech startups, and neo-digital challenger banks, many of whom are cloud native, will experience barriers to growth as a result of the lack of harmonisation across the EU. Finally, harmonising approaches to the cloud across jurisdictions will also help to facilitate the adoption of cloud at a Global level which creates efficiencies and encourages growth.

In addition, the adoption of cloud is also slowed down by the lack of clarity on the requisite uniform methods with which the banking sector has to comply in order to assess and ensure adequately the security and privacy. Not least to maintain trust and confidence of the financial system. If privacy and security measures are breached, the consequences will negatively impact the reputation of banks. What is more, they would most certainly be devastating for banks' customers.

Besides the need for harmonisation among EU financial supervisors outsourcing regulation, there is a need to bring agility to the cloud adoption process, reducing time to market to increase competitiveness.

In order to support and facilitate a responsible adoption of cloud computing within the banking industry, the European Commission should focus on efforts that support the creation of a clear and consistent regulatory framework at an EU and Global level, and guarantee a proportionate risk-based approach to due diligence and contracts between the Cloud Servicing Providers (CSPs) and the banking sector in respect of cloud computing in financial services.

Reference Directive(s) and/or Regulation(s): International and EU standards, national requirements regulating the outsourcing.

Proposed solutions

- **Recommendation 1: Support the creation of a clear and consistent EU and global regulatory framework**

  The European Commission should instruct the European Banking Authority (EBA) and the European Network and Information Security Agency (ENISA) to prioritise harmonisation across jurisdictions through the fast adoption of guidelines or an update of existing guidelines to ensure a common approach by regulators/supervisors regarding procedures and methodologies.

  There is a lack of common, internationally recognised standards for cloud computing as well as clarity (where needed) on how these should be applied to the use of this technology in the banking sector. This is also the case with regards to the rules imposed by the supervisors concerning the certification and audits for cloud governance and security. It is important that guidance coming from the relevant European agencies is quickly proposed to ensure the necessary harmonisation and guarantee legal certainty.

  The guidance should also facilitate the collaboration between the banking industry, cloud service providers, the regulators and national supervisory authorities to identify common best practices at EU level which will help banks meet regulatory compliance requirements and manage the technical security risks related to cloud adoption.

  To the appropriate extent, to bring further clarity on the existing rules/guidance available and applicable at EU level, the European Commission could create, with the support of the industry, a portal compiling all the existing legal instruments/rules available on cloud computing (ENISA, ECB etc.).

  Further consideration should also be given to ensuring a global level playing field in the rules governing the use of cloud computing in financial services. For example, less prescriptive regulations regarding the use of cloud computing, geolocation and data processing in non-EU countries (in particular the US) result in a competitive advantage for firms operating in those jurisdictions. EU institutions should thus move to create the conditions necessary for European firms to compete on a level playing field. This will result in positive competition creating growth and benefitting consumers.

- **Recommendation 2: Guarantee a proportionate risk-based approach to due diligence and to contracts between the CSPS and the banking sector**

  In order to guarantee a proportionate risk-based approach to due diligence and contracts between the CSPs and the banking sector, the European Commission should facilitate the establishment of a protocol on the transparency of risks by the industry. We propose the creation of a group of cloud experts, comprising providers and users, to elaborate such as protocol for 2017.

  Moving services to the cloud represents a systematic risk that was not present or was limited before (with other types of outsourcing). Large suppliers of cloud services can become a single point of failure when many banks rely their services on them.

This issue is exacerbated by the fact that many providers of special services rely themselves on the same platform IaaS/PaaS used by banks and their other providers, or use the services of the same SaaS providers.

Consequently, it is important to reach agreement between banks and CSPs upon the establishment of a protocol on the transparency of the risks which will mainly clarify regulatory oversight, right for auditing, liability issues as well as notification of breaches to supervisors and forensics' processes. General contract terms models, elaborated by both Banks and CSPs, should be established in the framework of this protocol to facilitate the integration of specific financial institutions' requirements.

This protocol should be a complement to the self-assessment conducted by the independent third party auditor and include:

- threat landscape (defined by the user);
- vulnerabilities (defined by the user and the cloud service provider);
- risk scenarios (defined by the users);
- risk treatment (defined by the users and providers) and adequacy evaluation;
- risk management governance principles (defined by the users and providers).

ISSUE 4:
DATA

Problems/issues

The ever-increasing possibilities on data storage and use (e.g. profiling, identifying patterns of consumption and making targeted offers) are revolutionising the way customers are served and businesses operate.

Given the changes in society and the use of social media, the new generations of customers arrive with fresh expectations. They might expect banks to take into account the data, already at their disposal, when offering services (with respect to data protection legislation). Some customers would even be willing to accept the sharing of data in order to have access to tailor-made products and services, benefits such as lower insurance premiums and purchase discounts or for instant access to them. Importantly, consumers expect banks to be able to deal with financial data in a highly confidential and trustworthy manner, as this has traditionally been the case.

On the other hand, there are challenges which may arise from the misuse of data, information asymmetries and data security. Such concerns are taken seriously by the banking industry, as trust and integrity are its biggest assets. Confidence in banks as trusted parties is essential for their reputation and business model, a fact which adds to the efforts and investments put into maintaining and improving set-ups ensuring the safety of customer data.

However, the benefits of digitalisation can only be reaped if each and every stakeholder adheres to the same high standard, and if the financial services' industry can apply data-based innovation in a clear regulatory environment that is the same for all players.

The recently adopted General Data Protection Regulation (GDPR) is one of the most advanced regulatory frameworks in the world regarding personal data protection, with high standard safeguards for consumers and their data. It applies widely, including situations where a non-EU company controls or processes personal data of natural persons who are in the EU. Although the banking sector supports the objectives of the GDPR to increase transparency around personal data processing and to give data subjects more control over their data, it is important to recognise that the greater level of prescription, compared to other economies, risks placing EU firms at a competitive disadvantage. The importance of having an appropriate competitive environment with a level playing field among all the different players - guaranteeing wide-ranging high standards and, in turn, enhancing consumer trust - should be a key reason for ensuring that not only banks have to comply with high standards in order to use personal data (e.g. in the case of data portability).

This level playing field needs to be achieved both:

- within the EU between different types of firms, e.g. banks and non-banks; and
- between EU and non-EU firms.

Stricter European rules should not unduly inhibit EU firms' ability from innovating, operating dynamically, using innovative data services and directing services to targeted market segments while their competitors from outside the EU serve European customers without similar restrictions. It is expected that the GDPR and the newly agreed EU-US Privacy Shield should hopefully be able to address part of this 'uneven level playing field'. Yet, care is needed to ensure that the potential of the European Digital Single Market can be realised, with EU firms able to innovate and compete not just in Europe, but internationally.

Seeing data as one of the most valuable assets in the digital world, helping European players to deploy the highest capabilities in data is essential to guaranteeing their competitiveness in the near future. The success of the Digital Single Market inevitably depends on it. As a result, any regulatory development in the field of data should ensure that players are allowed to extract value from the work they perform with data, while preserving data protection and privacy rights.

Further consideration should also be given to **enhancing the cooperation between the competent authorities regarding cybersecurity**, **data sharing** or to ensuring **further legal certainty in the interpretation of the GDPR.**

The following issues requires particular attention:

1. **Status of data and personal data portability**: Article 20 of the GDPR regulates the right to data portability.

   Data portability is central in order to provide customers with more choice, avoid data monopolies (competition issue) and allow personal data to be available to other operators (with consumer consent).

   The following two issues are however essential to resolve.

   a. **A clear distinction should be made between raw data and managed data:** raw data are those provided by the customer and managed data are those that have undergone further processing, such as verification, storage, cybersecurity checks, analysis, etc. These should belong to the companies that create an additional level of value based on their know-how.

      Banks (but also other operators) tend to enhance the quality of the raw data they receive from customers and other sources. In fact, they are often legally required to guarantee a higher quality of data (for AML, credit facilitation, etc.). These processes create an additional layer of value on top of the raw data. We believe it is important to recognize that there is an added value in the data managed by banks. When the customer applies for data portability, we believe that this **should only include the raw data that he/she has provided** in the initial process but not the data of enhanced quality that is the result of verifications and analysis.

      Should portable data include both raw data and managed data, it would mean that the right to portability would permit the free transmission of this added value enhancement delivered by banks. Consequently, both EU competitors and technology giants outside the European Union will unfairly benefit without any reciprocity.

   b. According to the GDPR, direct portability between data controllers will only take place when 'technically feasible'. Taking into account that the difference between raw data and managed data as well as the distinction of personal and non-personal data is already included in the GDPR. It should be clear that portable data means raw personal data directly provided by the customer. **Therefore, the terms "technically feasible" included in the GDPR need to be interpreted and implemented in a homogeneous way across EU Member States and industries**.

      It is also important to foster standardisation and direct portability between data controllers. There is an opportunity for the regulatory framework to ensure that the European financial sector has the right incentives to keep investing in validating the accuracy of data and enhancing data methodologies. If not, European banks will not be able to compete on an equal footing in the new digital era where data is a key driver of the business.

2. **Data breach notification**

The nature of security breaches/ incidents are such that often root causes and impacts hit not only locally. The incidents frequently need to be managed across groups of undertakings and jurisdictions. Banks are already today subject to strict requirements to notify security breaches/incidents to supervisory and competent authorities and other relevant bodies. With the introduction of the GDPR and the Directive on security of network and information systems (NIS) this number of competent reporting authorities is likely to increase.

For groups of undertakings with cross-border activities the number of authorities to notify is even larger. Owing to the need to address such important issues rapidly as well as the sensitive nature of sharing information about incidents, it is important that these processes be coordinated, and duplication avoided as much as possible.

In the case of a personal data breach, Article 34.3 of the GDPR specifies the conditions in which the communication to the data subject shall not be required. Nonetheless, there is **still a risk of alarming customers unnecessarily**. Investigating a suspected breach generally involves a significant amount of time and effort on the part of a data controller and it can take some time to determine exactly what has happened and who is affected, with the picture often changing as the investigation progresses.

It is therefore important to have a sufficient guarantee that the conditions for notifying/communicating the personal data breach to the supervisory authority or/and data subjects are feasible for banks (under the most expedient time possible). It would prevent legal uncertainties and ensure that authorities and data subjects be well informed without causing excessive burden for banks, or alarming victims of breaches unnecessarily (in particular avoiding confusion and 'notification fatigue' and disengagement among victims of breaches owing to notifications that do not pose material risks.). Most importantly, especially for the banking sector, notification to data subjects at all times may compromise the security of banks and facilitate financial crimes.

3. Data sharing with third country regulators and within a group

Exchange of data between authorities: financial institutions are often asked by European and non-European regulators for information that includes or relates to individuals who are customers, or employees of counterparties. This may be for the purposes of risk management, compliance, or investigations. This gives rise to data protection risks both within the EU and in the context of third countries.

Recently there has been greater emphasis placed on satisfying regulatory requests. Regulators expect their data requests to be satisfied, but if personal data is provided by a firm to a regulator without legal compulsion, or not as a result of legal obligation, then the organisation is at risk of breaching data protection law. Firms cannot easily impose conditions on disclosure or restrict onward transfer. Nonetheless, regulators (whether EU regulators or third country authorities) expect data requests to be complied with, and firms risk legal or regulatory action if they do not. There are also issues arising from freedom of information law in some jurisdictions where regulators can be asked to produce information on request.

Furthermore, in relation to transfers to regulators outside the European Union, these transfers need to be within the requirements of the third country transfer rules. However, given that regulators will not sign up to European Union Model Clauses, these transfers become problematic.

Exchange of data within a group: financial institutions often need to process personal data in the group of which they are members to achieve goals, such as offering a broader variety of products to the clients, or, efficiently tackling fraud.

Under the current Data Protection Directive, third country transfers between firms are broadly manageable, though not without complications due to the requirement for appropriate safeguards. The GDPR recognises in recital 48 a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. However, difficulties will be greater going forward for two main reasons.

1. The new provisions in the GDPR will make third country transfers more difficult as the possibility of making an internal adequacy decision is submitted to stricter requirements. In the absence of an alternative adequacy decision, data controllers will instead have to rely primarily on Standard Contractual Clauses for transfers outside their group. For intra-group transfers, firms will need to rely either on standard contractual clauses or on binding corporate rules (BCRs). However, we note that BCRs currently require 18 months or more to be approved and demand will likely increase under the GDPR.
2. There is uncertainty over firms' ability to rely even on the safeguards provided for under GDPR. The EU-U.S. Privacy Shield and Standard Contractual Clauses, for example, have an uncertain future, given the striking down of the Safe Harbour adequacy decision in 2015 and a more recent court challenge against Standard Contractual Clauses (SCCs)[4].

Reference Directive(s) and/or Regulation(s): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, EU-US Privacy Shield, Payment Services Directive 2.

Proposed solutions

- **Recommendation 1: Status of data & portability**

  As a part of its Free Flow of Data initiative the European Commission should collaborate with the Article 29 Working Party (and with the European Data Protection Board in due course) on portability . Clear EU guidance regarding the status of data - in particular for an homogenous and practical interpretation across industries on the portability principle - is fundamental. For example, Article 20 of the GDPR refers to the raw personal data, which has been input directly by the customer and has not been enhanced/verified or analysed further. Direct portability between controllers should be promoted. There should be a justification when there is no technical feasibility. [Common and workable interpretation of "technically feasible" for the portability of data between datacontrollers.] Ultimately, it should refer to the reciprocity of access to data between banks and non-banks.

  In order to guarantee an homogenous interpretation across the industry, call upon the European Commission to play a facilitator role in encouraging the Article 29 Working Party to have a continuous and open dialogue with the different stakeholders, in particular via the launch of a public consultation on portability.

[4] *Litigation Involving Facebook And Maximilian Schrems: on 31 May 2016, the Irish Data Protection Commissioner (DPC) commenced proceedings in the Irish High Court. The purpose of the proceedings is to seek a reference to the Court of Justice of the European Union (CJEU) in relation to the "standard contractual clauses" mechanism under which, at present, personal data can be transferred from the EU to the US.*

Call upon DG Connect to work closely with DG Justice - and in consultation with the industry - in assessing the consequences for the digital world and the competitiveness of the European Digital Single Market of the developments and interpretations of Article 20 of the GDPR.

The European Commission should exercise caution in considering possible changes to the rules around the 'ownership' of data, taking action only if clear market failures are apparent. Indeed, the concept of 'ownership' that is used when referring to citizen's rights in respect of data is a malleable and potentially inaccurate term for the rights that can be exercised over personal data by an individual, depending upon the individual and their circumstances.

- **Recommendation 2: Data breach notification**

Call upon the Article 29 Working Party and, in due course, the European Data Protection Board to provide guidance on the interpretation of data breach notification which should be clearly limited to relevant tangible and effective data breaches and excluded for potential data breaches. This guidance should be pragmatic, and principle-based taking into consideration the need to accommodate the specificities of different sectors.

Call for an active dialogue to be initiated and maintained between industry and the European Banking Authority and the European Central Bank in the context of the Single Supervisory Mechanism (SSM), and across other authorities and jurisdictions within the EU.
It should aim at:

- facilitating the implementation of the various incident reporting regimes in a coherent manner by streamlining harmonised processes to ensure alignment among local country guidance and avoid overlap and redundancy in reporting to multiple competent authorities under mutiple regimes (NIS Directive, PSD2, GDPR, SSM);
- sharing definitions and criteria to determine which major incidents should be required to be reported (this would allow comparability of data, evaluation of scenarios and extract lessons learned).

For the purpose of resilience and risk mitigation industry players need a legal framework which allows the possibility to share among themselves sensitive information related to fraud & cyber-attacks at national and cross-border level (data in general including personal data and risk data related to attacks/incidents).

- **Recommendation 3: Exchange of data between authorities & within a group**

Call for the development of a practical approach to the sharing of data by regulated sectors with regulatory authorities, both within the EU and in third countries. It would be helpful to include Memoranda of Understanding between the EU and third country regulators and authorities regarding the transfer of data between authorities. The European Commission and the European Data Protection Supervisor should facilitate and convene this work.

The Commission should continue its positive work under its Free Flow of Data initiative to remove diverging requirements among jurisdictions and ultimately call upon a clear legal basis to share information among jurisdictions at group company level.

ISSUE 5:
CYBERSECURITY

Problems/issues

The battle against cybercrime is of paramount importance in order to ensure the effective delivery of the Digital Single Market. Indeed, the trust of both citizens and companies in digital services and offerings cannot be taken for granted and must have the appropriate digital security. All efforts related to data protection and privacy are only as good as the security is efficient.

In this context, banks are on the front line in terms of cyber criminality (cyber criminals trying to steal not only money from the customers' accounts but also personal data). Moreover, the increasingly sophisticated and constantly evolving phishing techniques and the spreading of a multitude of banking malware variations require a continuous update of the threats' scenario.

In view of this, the banking sector has been investing heavily for many years in their IT infrastructure, as well as their customers' access to remote services, in order to minimize and prevent cyberattacks and frauds.

Cybersecurity is no respecter of borders. Rather, it is a global issue relevant to governmental, public and private sectors, in the same way that digital services interconnect various countries. As a result, collaboration, cooperation and convergence within and between the European and International levels are required. Cooperative actions among the interested stakeholders and bodies is essential in order to guarantee the highest level of customer and bank security. Efficient frameworks and networks for information sharing and reporting (threats, incidents, lessons learned, and countermeasures, avoiding unnecessary reporting burdens and overlap) are what is required. It is indeed essential to ensure that any conflicts with the General Data Protection Regulation[5] (GDPR) do not raise obstacles to the unfolding of an effective cybersecurity or hinder the exchange of relevant security-related information.

Finally, an important and essential component to cybersecurity is education. It is essential to continue to raise awareness and educate both citizens and businesses on cyber risks.

Reference Directive(s) and/or Regulation(s): network and information systems Directive[6] (NIS) (2016/1148); NIST Framework; Payment Services Directive 2 (PSD2) (Directive EU 2366/2015), Chapter V; Data Privacy Directive; National Banking Regulation on critical infrastructure and Business Continuity.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Proposed solutions

- **Recommendation 1: Incident reporting**

Streamlining harmonised format and procedures for security (IT) incident reporting to avoid overlap and redundancy in reporting to multiple competent authorities (NIS Directive, PSD2, Data protection regulation, Single Supervisory Mechanism SSM).

- Share definition and criteria to determine the major incident to be reported (this would allow comparability of data, evaluation of scenarios and drawing the lessons learned).
- Set common and homogeneous criteria to understand the level of significance and severity of a security incident.
- Harmonise the different formats and procedures for incident notification, in order to avoid redundancies; in this regard, the aggregation of incident notification in a single point of contact would be very much supported.
- Establish a constant dialogue between the European Central Bank in the context of the Single Supervisory Mechanism (ECB/SSM) and the relevant stakeholders (banks, banking associations, European Banking Federation, etc.) on methodologies/processes for incident reporting and cyber risk assessment.
- Establish a worthy mechanism able to extract and distribute to banks, lessons learned, deriving from incident reporting, in order to support incident and fraud prevention and early warning.

- **Recommendation 2: Information sharing**

- The Banking industry for its resilience purpose and risk mitigation needs a legal framework which allows the possibility to share among themselves sensitive information related to fraud & cyber-attacks at national and cross-border level. For this purpose, the banking industry would call upon an active dialogue between the industry, the Article 29 Working Party (EU Data Protection Board), European Banking Authority (EBA) and the European Central Bank in the context of the Single Supervision Mechanism (SSM) with a view to assessing how best to enable this sharing of relevant (including possibly sensitive) information, possibly drawing on the experience from the newly established private initiative of the UK Cyber Defense Alliance.

ISSUE 6:
PLATFORMS

Problems/issues

The European Commission defines platforms as "two-sided markets where users are brought together… in order to facilitate an interaction (exchange of information, a commercial transaction, etc."). Some of the most successful and fastest scaling businesses of the last decade – Google, Facebook, Apple, Uber, and Airbnb – are built on the platform business model. These businesses create a plug-and-play infrastructure that enables producers and consumers to connect and interact with each other in a manner that was not possible in the past. The direct interaction between users and providers of products and services offered by these platforms give consumers and companies what they want, when they want and in a format they prefer (choice, affordable products, fast delivery). In short, platforms change the very design of traditional business models and marketing activities.

Digital platforms will have a profound impact on financial services, **since they completely reshape the relationship between the providers of financial products and the end-users**. As seen in other sectors, markets in which digital platform models have a significant role, tend towards concentration due to the huge economies of scale and the accumulation of customer data. Consequently, the emergence of platforms in the financial sector will inevitably face organisational, regulatory and competition issues.

In the context of the analysis that the European Commission is performing on the Role of Digital Platforms and the determination it will show on whether additional EU action is needed by spring 2017, we would like to include a number of comments.

Concerning the Free Flow of data initiative

The European Commission is aware of the challenges ahead, and has highlighted the benefits of users being able to switch platforms as easily as possible. This is regarded as a means to guaranteeing that the quality of the service provided, and not lock-in strategies, is the main driver for consumer choice. As part of the 'free flow of data' initiative, DG Connect has stated that "it will consider options for effective approaches, including technical standards, to facilitate switching and portability of data among different online platform and cloud computing services, both for business and private users".

We support this initiative, as it would imply a reciprocal treatment, given that such technical standards already exist for banks in the context of Payment Services Directive 2 (PSD2). Indeed, by 2018, all Account Servicing Payment Service Providers (AS PSPs) will have to share an extremely valuable set of personal data (account information) with third parties registered as Account Information Service Providers (AISPs) if the clients request so. Most importantly, this access will be standardised and, eventually, take place over a pre-defined set of APIs.

At the same time, the General Data Protection Regulation (GDPR) recognizes a right to personal data portability (see data issues for the limits on data portability). Even for the portability of what we define as raw data, the GDPR will require that all data controllers share sets of personal data provided by the data subjects - should they individually request so - with the data subjects themselves (with a third party only when considered "technically feasible") and using a "structured, commonly used, machine-readable and interoperable format". The main difference with the framework applied to financial institutions under PSD2 is that GDPR "should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible" (Recital 68 of the GDPR).

If the European Commission believes that the standardized format to access certain customers' raw data could be a trigger for better services, as it has decided for PSD2, it would be logical to extend this to the rest of sectors. Otherwise, the combination of PSD2 and GDPR will lead to a most probable scenario in which, by 2018, all European banks will have to grant access to their individual clients' transactional data (which are also a type of personal data) using a standard access to account interface that can be easily used by digital players, from both inside and outside Europe. On the other hand, if any European bank wants to gather personal data from its clients from any other data controller, even big digital providers located outside the EU, these are only obliged to provide a structured, commonly used, machine-readable and interoperable format, but each of them might use a different format and only allow our clients to download a heavy file, negatively affecting customer experience.

Through the large scale of products and services offered and their internal data mining, large operators of digital platforms (Google, Amazon, Facebook, Apple) already have a lot of information on European customers (social network, place of residence, composition of the family, spending patterns, purchasing habits). Their infrastructure and data base will allow them to anticipate their clients' needs, offer off-the-shelf products and services, in store or online in a way that excludes any other operators from competing. This situation may result in a complete customer lock-up that runs against all the objectives of the Digital Single Market as set by the European Commission.

The European Commission has also declared its intention to analyze relations between platforms and their suppliers or partners in order to assess, and map out, the nature and extent of problems which could result in harm to these suppliers' business activities, in particular where this may negatively affect innovation.

In this context, as per the Commission's "Communication on Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe", there is an opportunity for the European Commission to develop a clear strategy regarding the platforms' ecosystem to make sure that European players are able to extract value from their innovation.

According to the European Commission, Europe is an important global player in app development (in 2013, EU developers accounted for 42% of global consumer app revenue). Moreover, Europeans have already surpassed US consumers in terms of apps downloads. However, digital platforms - which are mainly based outside the EU - are the ones that extract most of the value from this innovation.

A study by Gigaom for the European Commission found that in 2013 EU developers took in EUR 17.5 billion in revenue and it was forecasted to increase to EUR 63 billion in 2018. In addition to EUR 6 billion from app sales, in-app spending for virtual goods and advertising, EU developers recognized EUR 11.5 billion in 2013 from contract labour. However, the overall EU trade balance of the app economy is negative (-EUR 128 million). This is mostly due to the app platform fees that EU developers pay on revenue earned.

By spring 2017, the Commission will determine whether additional EU action is needed. We welcome this initiative as it seems critical for European future competitiveness in the digital world that the European players are able to benefit from the value they create.

Some digital platforms have acquired colossal dimensions and reach. And given customers' demands and for customer convenience European providers cannot avoid partnering with them. However, these providers' bargaining power is immense and European companies need to be ready to accept any contractual conditions in order to use their services. The European Commission should make sure that digital giants cannot impose contractual clauses that prevent the European companies from enjoying a fair share for the value they create.

The European Commission also has an opportunity to make sure that the responsibility burden is correctly allocated. In all the cases where the role of the platform provider goes beyond the mere operation of a marketplace, and includes the provision of services such as payments' processing, authentication, etc., for which it makes a profit, the platform provider should bear similar responsibilities as other players that

are not organized under a platform structure. Platforms should not use their bargaining power to include clauses for systematic exemption of a responsibility that is compulsory for other players.

A good example is PSD2, where the draft Regulatory Technical Standards (RTS) on customer authentication and secure communication includes a provision to set contractual agreements between Payment Services Providers and Account information services providers outside the scope of PSD2 (and thus, outside the responsibilities assigned by the regulation). We believe that, beyond the concrete example of PSD2, which is now under the scope of the European Banking Authority (EBA), the Commission has an opportunity to avoid a situation in which platforms operators can use their bargaining power to impose such conditions.

The unbalanced power of platforms also has negative consequences for European consumers: in many cases, digital platform operators apply a different treatment to applications provided by other providers than to their own (i.e. proprietary apps pre-installation, slower external party application validation, or even denying access to certain functionalities for third party applications, based on hardware restrictions). This limits customer choices and forces any third party who wants to offer a service to reach a commercial agreement with the hardware manufacturer.

In short, the EU Commission should be careful not to provide non-EU players with all the tools (access to customers' data, absence of responsibilities etc.) at the expense of EU entities (including banks) which in the end will need to continue guarantying the systems' safety and necessary investment levels.

Reference Directive(s) and/or Regulation(s): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM (2016)288). Published on 25/05/2016: Commission Staff Working Document on Online Platforms, accompanying the document "Communication on Online Platforms and the Digital Single Market" (COM (2016) 288). Published on 25/05/2016.

Proposed solutions

- **Recommendation 1:**

  The European Commission, with the help of the Article 29 Working Party, should develop clear EU guidance regarding the interpretation of the portability principle (see Issue 4, recommendation 1 above).

- **Recommendation 2:**

  More generally speaking, the complexity of issues raised by the scale of digital platforms calls for a holistic approach that puts a strong emphasis on the protection of consumer and corporate data, both general and sensitive.

- **Recommendation 3:**

  We agreed with the European Commission that further analysis is required to identify the most appropriate solutions to address the issues listed above, in close collaboration between market operators. In this analysis, specific attention should be given to:
  - the allocation of responsibilities between the platforms and third parties, assessing whether it be necessary to include basic principles that cannot be decided by contractual negotiation;
  - assessing whether EU companies and developers can negotiate in balanced conditions so that they enjoy a fair compensation for the value they create;
  - where vertical integration exists, i.e. where the platform directly competes with third party companies offering products and services though the platform, establish clear rules to avoid platforms discriminating against other providers.

ISSUE 7:
PAYMENTS

Problems/issues

For many years, the European payment industry has offered the most secure payment environment to consumers and merchants alike for two main reasons: i) any new product and service launched is natively conceived in a very secure way and, ii) once these products have been launched on the market, payment providers have adopted internal processes that allows them to prevent or react in a very agile way to any fraud attack.

The Payment Services Directive[7] 2 (PSD2) aims at reinforcing the overall security framework for payments in Europe and mandates the European Banking Authority to develop standards that are deemed to be based on "effective and risk-based requirements" and "allow for the development of user-friendly, accessible and innovative means of payments" (article 98.2.d)

The draft Regulatory Technical Standards (RTS) published by the European Banking Authority (EBA) on 12 August 2016 are however very prescriptive and likely to make it more difficult for payment providers to apply or introduce specific policies or tools based on their risk analysis and offer payment products that are user-friendly.

Today's market reality shows that authentication methods for purchasing online can differ from one transaction to another, depending on the security protocols implemented by e-merchants, the amount of the transaction or the environment within which this transaction takes place. Risk profiling based on device, IP recognition and behavioural analytics becomes more sophisticated by the day. The draft RTS proposed by the EBA introduces a major change to the PSD2 (Article 74.2) as it imposes strong customer authentication for all online transactions above €10 as from October 2018. Article 74.2 clearly allows Payment Services Providers (and payees) not to require strong customer authentication provided that any financial damage resulting from an unauthorised transaction is refunded to the payer. This "shift of liability" has been in place for more than 20 years as part of the EMV standard and has allowed merchants to adopt their own risk management processes that have proved to be quite effective over time and a useful complement to the processes put in place by PSPs.

The legal regime under PSD2 makes banks liable in the first place towards the customer in case of fraudulent, wrongly or non-executed payment transactions, even if the payment was initiated through a payment initiation services' provider. Therefore, any exemption to apply strong customer authentication should not be mandatory on ASPSPs.

The European Union cannot deprive itself of this myriad of methods as they offer the right balance between security and customer convenience. At a time when European citizens can benefit fully from digitalisation in their daily lives, it would be regrettable to discourage them from using state of the art technologies.

Equally, many use cases will have to be redesigned to fit the RTS requirements without any demonstrable security benefit as two examples illustrate herewith.

- All physical card transactions will be subject to passwords, even for very small amounts. As a result, all parking and tollways terminals will have to be replaced to allow for a password entry. Customer convenience will be dramatically impacted with limited if not no security benefit.

[7] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

- The ease with which mobile payments can be made today, where the payer has only his/her mobile phone to make a payment, will equally be affected by the very stringent requirements proposed by the European Banking Authority. Requiring the segregation of channels, applications or device for initiating a payment and receiving the authentication code will introduce an over complicated process for users, forcing them to go from one application to the other, eventually completely discouraging them from using their mobile device for payment transactions. Security experts are extremely doubtful as to the merits of the segregation imposed by the RTS as it could multiply the attack factors, compared to, for example, integrated end-to-end encrypted processes.

In addition to that, PSD2 will apply from 13 January 2018, while the final RTS are not expected before October 2018 at the earliest. This nine-month vacuum will inevitably lead to a fragmented approach on the access to Payment Accounts by third party providers (TPP), with various liability regimes and, most probably, no Qualified Authority to manage the entire process. In other words, PSD2 and the draft RTs require the whole payment industry to create an entirely new landscape but the most basic tools to make it secure, seamless and open are likely to be missing at the time of implementation.

Another important requirement of the PSD2 is that payment services providers (PSPs) should identify themselves when they initiate a payment transaction or provide account information service. We are concerned that the proposed solution in the draft EBA RTS (based on eIDAS) may not be available in the market by the date the RTS will be applicable.

Reference Directive(s) and/or Regulation(s)

Proposed solutions

Flexibility and adaptability is of the essence in the payment industry and should be maintained. Herewith are the points we would advocate:

- **Recommendation 1:**

  Introducing **a risk-based approach that allows PSPs to protect their clients' assets** (clients and corporates alike) by giving them the requisite flexibility needed to react immediately to new fraud trends and work closely with law enforcement agencies to share data and intelligence. The exemptions proposed by the EBA to the strong customer authentication should therefore be reviewed. At the same time, ASPSPs should not be obliged to apply the exemptions.

- **Recommendation 2:**

  To **maintain the liability shift provided in Article 74.2 PSD2** when strong authentication is not applied, provided that users are protected from unauthorized transaction and the merchant or its Payment Service Provider accept liability in case of fraud.

- **Recommendation 3:**

  To **set high-level standards to which ASPSPs can adapt in a flexible manner**, depending on the environment or specific cyber threats at a given moment in time. These standards could relate to the PSU's device, the communication, application, payer and payee profiling, transaction level (to go online or not), Interpol warnings, merchants' own authentication processes, in line with option 1.1 referred to earlier. For a long time indeed, merchants have been closely associated with the fight against fraud and some e-merchants have adopted very sophisticated tools to identify their clients and carry out a risk assessment on a case-by-case basis. Some have elected not to apply strong customer authentication and agree to be fully liable in case of an unauthorised transaction.

- **Recommendation 4:**

To call the European institutions (European Commission, European Central Bank and European Banking Authority (EBA) to support solutions developed by ASPSPs allowing a sound and well-functioning **communication infrastructure between ASPSPs and Third Party Providers (TPPs), aiming at ensuring both customers' protection and TPPs' activity.**

- **Recommendation 5:**

To call upon the EBA and European Commission to promote a common and consistent approach on the access to payment accounts by TPPs. The time gap between the application of the PSD2 and the application of EBA Strong Customer Authentication (SCA) Regulatory Technical Standards (RTS) should be addressed having at EU level a clear liability regime and timeframe.

- **Recommendation 6:**

Foster the availability of an adequate eIDAS solution on the market to identify Payment Initiation Services Providers and Account Information Services Providers by the time the European Banking Authority RTS 's become applicable.

ISSUE 8:
EU FRAMEWORK FOR EXPERIMENTATION

Problems/issues

Banks are seeking to test out new technologies, solutions and business models but are constrained by the existing regulatory framework which does not allow low-risk and low-scale experimentation to take place under less stringent rules. This issue limits competition and may stifle innovation in financial services. Consumers, in turn, are hindered from enjoying certain improved value propositions from their trusted banks.

Regulators could help by exploring how to gear up in order to support innovation across its activities, working with industry and wider stakeholders. A risk-based approach to regulation should be consistent throughout the innovation lifecycle, providing an appropriate, flexible and simplified regulatory framework for both incumbents and new players to experiment with new technologies and business models in interaction with regulators. Such an approach would allow regulators to understand more thoroughly the benefits and risks of new services before they assess the validity of the current regulatory framework. A first step on this journey is to consider the creation of an EU framework for experimentation.

There are already a number of initiatives taking place in several countries. For example:

- the British Financial Conduct Authority (FCA) has launched a scheme called the UK Regulatory Sandbox; in this formula, consumer protection and full control of new models under trial must be ensured and results duly communicated to regulatory authorities; firms – large and small – could apply for the first cohort of the regulatory sandbox up until 8 July 2016 and the application period for the second cohort will begin on 21 November 2016;
- the Monetary Authority of Singapore (MAS) released a Consultation Paper on Fintech Regulatory Sandboxes Guidelines on 6 June 2016; although the Singaporean approach is similar to the UK's, MAS has also asked larger financial firms to provide 'problem statements' which could then be tackled by startups;
- the Hong Kong Monetary Authority recently announced the creation of a "Fintech Supervisory Sandbox" as well as "Fintech Innovation Hub" to promote new technology;
- the Australian Securities and Investments Commission recently launched a consultation on its document "Further measures to facilitate innovation in financial services" and "Regulatory sandbox licensing exemption";
- the United States just proposed a Bill aiming at setting up a 'Sandbox' for Fintech Innovation.

The expected outcome of the framework for experimentation should be a learning process in which a company successfully delivers an innovative new product or service while working with the regulator on how to apply existing rules in a new area, which in some cases could lead to new regulatory or supervisory approaches. Prior to accepting the project, it is important to analysis to determine whether the project's success does not rely on changes of regulations beyond those made by the authorities in charge of the jurisdiction. Otherwise, it will be impossible for the project to enter the wider European market. This is why a combination of both national and European framework is ideal..

Proposed solutions

- **Recommendation 1:**

We call for the EU Commission to consider the adoption of a framework for experimentation (Europe-wide approach on sandboxes) at European level which would avoid creating additional fragmentation in the single market and distortion of competition between operators in Europe. If appropriately implemented, it can make a significant contribution to innovation in financial services to the benefit of consumers.

A **three-step approach** could be followed.

1. As a first step we recommend that the European Commission issue a first document in which it states the need and potential benefits of a framework for experimentation for European citizens and firms, as well as how to address the coordination challenges linked to the different regulatory and supervisory bodies involved.
2. The second step should be that with minimum delay national regulators' share across Europe best practices which facilitated the implementation of successful innovations.
3. In the end, the final output should ideally be harmonised tools that avoid national divergences in implementation and establish a level playing field for all countries and participants. A harmonised framework for experimentation would, additionally, foster innovation in cross-border services, in line with the Digital Single Market.

Regarding the process: to avoid discretionary decisions, clear and harmonised criteria for projects to enter the framework for experimentation have to be defined and made publicly available. These criteria must define the requirements of eligibility for the applicant, and a number of key issues that the project must meet prior to application. For example, previous research and a testing plan that includes milestones, how to measure its success, testing parameters, customer and general safeguards (for data protection, security and confidentiality measures, e.g. data anonymisation, limited and monitored access to the framework for an experimentation environment, etc.), risk assessment and exit strategy. It must also include a check on ethical purposes, exclude certain particularly sensitive data and identify the volume of data that will be concerned. And, finally, the proposed project must be innovative with a short duration and verify that there are not similar products or services already on the market where the framework for experimentation operates. Multi-stakeholder projects should also be considered.

The approval process must be able to accept regulated companies and non-regulated companies. The latter will be able to test their projects but must accomplish a minimum set of guarantees to ensure a level playing field with established players. As soon as those companies enter the market all players must follow all the rules which apply to them. The scale of the activities carried out within the sandbox has to be limited to avoid additional risks to the financial system and to consumers. The authorisation process has to be simple and transparent and there have to be waivers (e.g. no enforcement letter or specific guidance.) or amendments to particular rules if testing activities would otherwise breach them. Finally, once the experimentation is running, a clear supervision process must be established to guarantee that the testing company addresses the agreed milestones (success and failure for a project's testing should be clearly defined before testing begins), otherwise the appropriate penalties must be applied.

ISSUE 9:
DIGITAL SKILLS

Problems/issues

There is no doubt that digitalisation is a great opportunity for the European economy, for competitiveness, new services and innovation but there are challenges to be addressed, particularly the need to develop digital skills and lifelong learning, to re- and up-skill people for new or changing jobs.

At the same time, there are currently 23.5 million unemployed persons across Europe, of which 4.7 million are young people. We know that digitalisation leads to the automation of certain routine tasks and while many jobs are changing, some are disappearing. This is also the case in the banking sector. At the same time 37 % of the workforce in Europe have insufficient digital skills. Only 25% of students are taught by digitally confident and supportive teachers with access to ICT and low obstacles to their use at school. Employment of ICT professionals in the EU has risen by 4% on average a year over the past 10 years, yet 39% of enterprises trying to recruit ICT professionals have difficulty doing so.

The financial sector is affected by all of these digital skills gaps and:

- has to compete with the ICT sector for talent in a number of ICT areas such as cybersecurity, big data and artificial intelligence sector;
- has a key role to play in retraining our workforce with a lifelong learning perspective;
- need to work with education providers to contribute to a better match between curricula and industry needs;
- can raise awareness and support training its customers (European citizens) in digital skills;
- face a situation where some traditional roles of its employees are either changed or sometimes replaced by machines;
- has its services increasingly delivered online.

Proposed solutions

- **Recommendation 1:**

Many Banks are willing to commit to take action by signing up to the membership charter for the Digital Skills and Jobs Coalition and work closely with the Coalition's stakeholders to address the lack of digital skills in our society and digitalisation's impact on jobs. This is achieved by:

1. signing the membership charter to become part of the coalition and declare the intent to act in line with the points below (within one or more of the following areas; i. increase the number of ICT professionals; ii. reskill the general workforce; iii. increase the level of digital skills for all citizens and iv. modernise education);
2. presenting previously taken actions in line with the membership charter that can act as best practices and be replicated or scaled up throughout Europe;
3. presenting new actions in line with the membership charter; these actions will be annually followed up by the Commission.

- **Recommendation 2:**

The EBF would also add digital education as a component of its activities on financial education, notably in the context of the activities around the European Money Week (EMW), initiative launched by the EBF more than two years ago (www.europeanmoneyweek.eu).

CONTACT PERSONS:

WIM MIJS

Chief Executive

SEBASTIEN DE BROUWER

Executive Director
Retail, Legal, Economic & Social Policy

s.debrouwer@ebf.eu

NOEMIE PAPP

Senior Policy Adviser
Digital & Retail

n.papp@ebf.eu

PASCALE-MARIE BRIEN

Senior Policy Adviser
Payments & Digital

p.brien@ebf.eu

European Banking Federation aisbl
Brussels / 56 Avenue des Arts, 1000 Brussels, Belgium
Frankfurt / Weißfrauenstraße 12-16, 60311, Germany

www.ebf.eu **info@ebf.eu** **#ebf**