

#ebfdigitalbanking  
[www.ebfdigitalbanking.eu](http://www.ebfdigitalbanking.eu)











# Driving the Digital Transformation

The EBF blueprint for digital banking and policy change

# Contents

Foreword	3
About the EBF blueprint	6
Banks increasingly turning digital	8
EBF key messages	15
Key Recommendations	17

	Better access to digital banking products and services	19
	Data value chain / Big data	23
	Digital payments	27
	• Mobile & instant payments	27
	• E-invoicing	30
	Cybersecurity	33
	Crypto-technologies	36
	E-identification / e-signature	39
	Digital skills	43
	• Competencies & talent recruitment	43
	• Digital Education	47
	Removing regulatory inconsistencies	50

## Foreword: We believe in digital

I am a great believer in digital. For me my life is digital. If it is not on my phone it does not exist. All of our lives are becoming more and more digital. This is what brings growth to our economy.

As the European Banking Federation we are also a great believer in the European Commission's plans on the Digital Single Market. We are keen to assist and support this strategy. That is why we wrote this blueprint. It is also written as a digital report, not a bulky one with a grey cover but with a fresh design, infographics and multimedia. All you need to know is available here, online.


The Digital Single Market will only work if we have a high level of consumer protection, if there is trust among companies, SMEs, banks, institutions and governments, and if we have regulated our privacy in a satisfactory way. We also have to protect ourselves against cybercriminals. We have to unite with each other against cybercrime.

If we achieve these goals then the Digital Single Market will be a success. This blueprint describes the dilemmas. It offers solutions for the important aspects that need to be addressed.

So please read on. Of course we are interested in talking to the Commission, the institutions, the Parliament, and the Member States. But also to you, dear reader. The Digital Single Market is there for us all. You know where to find us if you have feedback. We are keen to hear your comments.

**Wim Mijs**

Chief Executive, European Banking Federation



***"If it is not on my phone it does not exist. All of our lives will be more and more digital. This is what brings growth to our economy."***



## Banks in the driving seat

 **€62.000.000.000**

European banks are major investors in IT infrastructure and services, pouring billions of euros every year into innovation, research, as well as maintenance.

Research among banks conducted in 2015 by Celent shows that European banks in 2018 expect to invest some €62 billion in IT.

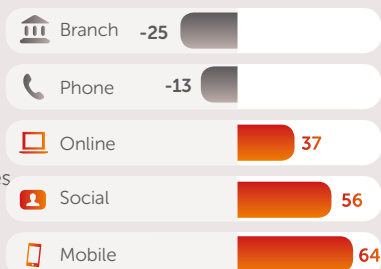
***"New technology is changing the face of financial services. It will be an important driver of the integration of capital markets."***

**Jonathan Hill**  
European Commissioner  
for Financial Stability and  
Capital Markets Union

### Anticipating disruption

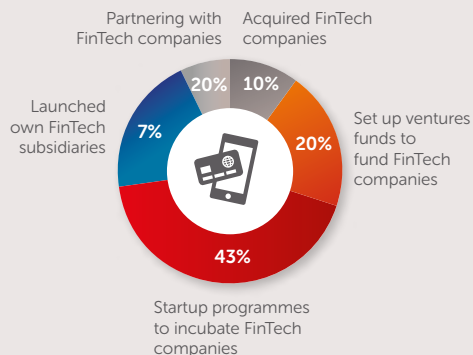
Bankers have been expecting major changes in customer channels

This survey among bankers by PWC estimates the approximate percentage change of the activities on various customer channels in 2013 and 2016:



### Banks embrace the FinTech opportunity

European banks lead the engagement with FinTech companies, according to analysis by blogger Avinash Swamy, as reported by thefinanser.co.uk.:



## Customers at the centre

 **214.000.000**



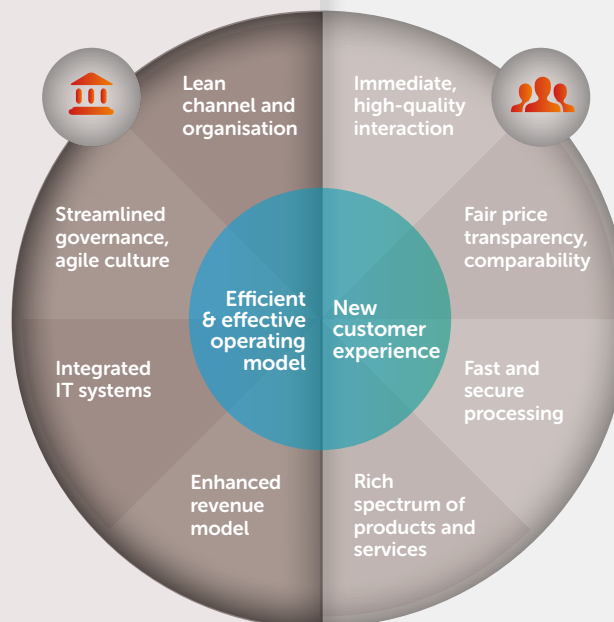
Some 214 million people in Europe will use mobile banking services by 2018 according to Forrester Research.

Approximately 185 million Europeans expect to use a mobile payment app instead of cash in 2016. The value of mobile payments worldwide is set to exceed €207 billion in 2015, according to an Ipsos survey conducted on behalf of a bank.

***"Helping customers understand their money... will instill a level of control and confidence."***

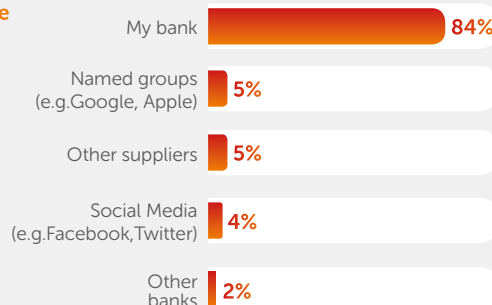
**Benjamin Ensor**  
Forrester Research

## Benefits for both



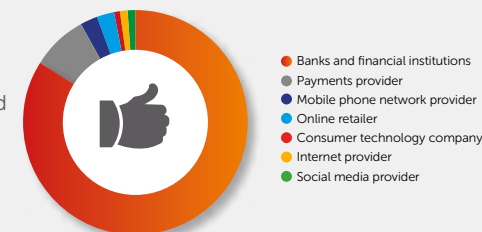
### Preference for mobile payments

Most respondents in a 2015 ING survey said they prefer their own bank over other online services when conducting mobile payments:



### Customers trust banks with their data

Banks are the type of company most trusted to securely manage customer data, according to a study by Accenture:



**315.000.000 users**

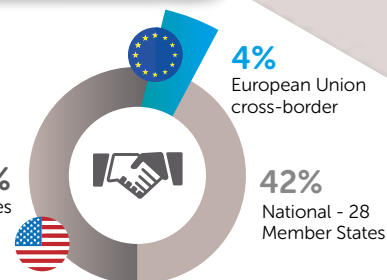
Some 315 million Europeans use the Internet every day according to Eurostat.



## Digital Single Market

EU cross-border services account for **only 4%** of today's digital market in Europe:

54%  
United States



**15%** of European consumers bought online from other EU countries in 2014:



**€415.000.000.000**

**3.800.000 jobs**



The Digital Single Market can create up to €415 billion in additional growth, with as many as 3.8 million new jobs and a vibrant knowledge-based society, according to the EU Commission.

*"You can't use 18<sup>th</sup> century law for a digital world."*

**Andris Ansip**,  
Vice-President in charge of Digital Single Market, European Commission

**7%** of SMEs sell cross-border in the EU single market:



## What you need to know

1

Banks are a natural and strategic partner for Europe's economy and for a successful Digital Single Market.

2

A holistic approach is necessary to ensure the EU regulations are adjusted to digital market reality.

3

Banks support a competitive, innovative Digital Single Market with trust, security and consumer protection.

4

A strong Digital Single Market requires strong cooperation in the fight against cybercrime.

## About the EBF blueprint

The banking sector is much more than an industry and more than an employer. Banks represent strategic partners for Europe's economy. They channel savings to investments to ensure economic activity and growth and provide essential services in a secure and reliable way for their customers, consumers and corporates alike: deposits, lending, distribution and access to funds, financial advice and payments, among other products and services. Today, they fulfil a vital role in the economy, not to mention that they have always been used as a tool for public policy, and it will still be the case in the future (e.g. transmission channel for monetary policy and access to finance). In this way they play a key part in society and distinguish themselves from the other players.

The emergence of new technologies such as cloud-based systems, high-speed wireless network, biometrics or instant payment systems is leading to more efficient banking services, generating many new opportunities for banks and better products and services for their customers. If banks are sometimes perceived as 'conservative', they are actually highly innovative actors, constantly embracing change over the years. In this respect, the current digital revolution is simply another significant step in the history of banking.

Digital banking is often understood to be the use of mobile banking or online payments but its meaning is much broader. It encompasses the ability to interact digitally with customers. This is done by integrating digital technologies (e.g. through the use of strategic analytics tools such as big data, social media, innovative payment solutions, mobile technology) and by providing services through digital channels in real time, a seamless experience with appropriate security and authentication systems. Digital banking is, in fact, all about improving the customer experience.

## The aim of the EBF Blueprint

The European Banking Federation's (EBF) Blueprint on Digital Banking aims at helping to understand more effectively the digital transformation initiated by banks. The EBF Blueprint focuses on the challenges and opportunities in retail banking. It also explains why banks should be considered as strategic players in the Digital Single Market (DSM).

With the aim of encouraging discussion and reflection among banks and EU policy makers, the EBF Blueprint proposes recommendations on which to build a proper framework for a workable DSM. Recommendations, to ensure that the reforms undertaken will lead to the desired effects: restoring trust, creating a competitive and innovative market, and boosting economic growth and employment.

In particular, the EBF blueprint provides indications on the changing environment driven by customer expectations, a description of today's digital bank representing an innovative customer experience, and a portrayal of the bank of the future. And more importantly, the barriers and opportunities for banks and their customers linked to some fundamental issues: better access to banking products and services, big data, payments (mobile/instant and e-invoicing), cybersecurity, crypto-technologies, e-identification, digital skills (education, competencies, recruitment), and the importance of removing regulatory inconsistencies and ensuring fair competition.

As a next step, the EBF Blueprint will be followed by 'issue papers' proposing an in-depth analysis on the strategic topics identified.

***"New technology is changing the face of financial services. It will be an important driver of the integration of capital markets. Examples like electronic trading, crowdfunding and FinTech show this."***

Lord Jonathan Hill  
COMMISSIONER FOR FINANCIAL  
STABILITY, FINANCIAL SERVICES  
AND CAPITAL MARKETS  
UNION, EUROPEAN COMMISSION

## The role of the European Banking Federation

In light of the rapid emergence of digital banking services, the banking sector is placed at the centre of this digital transformation.

The European Banking Federation (EBF), as representative of the European banking industry, is committed to accompanying banks in this transformation. Namely, to discuss with European institutions the reality of a regulatory environment conducive to establishing secure, reliable and efficient digital banking services. In addition, the EBF, in its commitment to generating a single market for financial services and to supporting policies that foster economic growth, is the obvious strategic partner in the creation of an ambitious Digital Single Market.

The EBF, as the voice of the European banking sector unites 32 national banking associations in Europe which together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.5 million people. EBF members represent banks which make loans available to the European economy in excess of €20 trillion and securely handle more than 400 million payment transactions per day.

# Banks increasingly turning digital

The digital transformation of financial services is led by many trends.

## The development of new technologies

The swift development of new technologies, Internet, smartphones and tablets in less than 10 years and the challenge of new entrants (operating digital-only products and services) and new models, adds a new dimension to the changing role of banking. Technology companies and start-ups rapidly expand their activities to financial services, continually innovating and competing – or collaborating – with banks and other financial institutions in various segments of the financial markets or in activities that do not specifically require a banking licence. This contributes to pushing banks to rethink the way they operate.

## The change of customer expectations

The change is also coming from new customer expectations. Today's customers are not the same as they were ten years ago. Their expectations towards products and services have changed in just a few years. Digital consumers belong to the digital native generation, born and raised with Internet: the Generation Y (born between 1977 and 1994), considered remarkable technology wise, exposed to technology since early childhood and impervious to most traditional marketing; and the Generation Z (born in the mid-90s to early '00s), accustomed to a media and online environment in which options are virtually limitless.

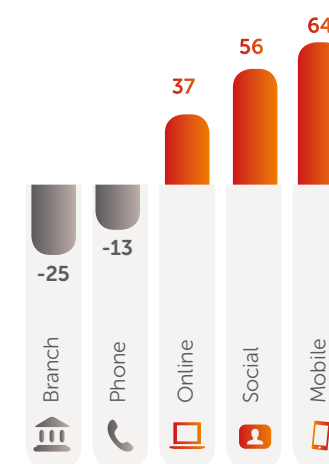
Both generations are extremely connected and rely heavily on smartphones/apps and even wearables to enjoy the best customer-experience or benefit from the most popular content. They adapt quickly to new changes and continually seek information or advice on the Internet or social networks. These digital consumers demand more choices, immediate availability and direct access to ready-to-use information and services. They expect fast, safe and simple banking products and services. They want banks to provide more than mere transactional services and expect them to understand their needs and to act as trusted advisers.

At the same time the major milestones in life - from birth to retirement - remain unchanged and faced with these landmarks, consumers continue to make financial decisions. What changes, is the way they approach these decisions. Consumers still shop around for the best services but when comparing and applying for loans, mortgages and credit cards, the majority of them are now using Internet instead of visiting a bank branch.

The way we bank now has considerably changed.

### Disruption anticipated Bankers expect changes in customer channels

Thinking of your total customer distribution, what approximate percentage of your customers is active on the following channels today and how many do you expect to be active in a few years?



● Percent change anticipated, 2013-2016  
(Source: PwC's Global Digital Banking Survey, 2013)



## Innovation: the leading trend for the best customer experience

In order to meet customer demand, banks continually launch, high quality digital communication, user-friendly financial products and services that simplify consumers' trade and transaction management experience. They lead the change through innovative solutions but successfully preserve their core values: trust, integrity, privacy and security to offer the best of the digital age to consumers.

Today, banks propose more 'tailor-made' customer experiences with products adapted to consumer needs: new designed apps to manage their finance, benefit from discounts (in certain shops) and have instant access to their accounts. Banks' websites, especially online banking sections, are now required to offer a pleasant experience while remaining highly functional. This necessitates rich content including elegant designs, instant search results and interactive features.

The innovative solutions developed by banks aim to create a customer experience which is translated in practice:

### ■ From a multichannel to an omnichannel approach

Until recently, most customers banked through multiple channels: going to branches to access products and services to explain their needs; using an Automated Teller Machine (ATM) to withdraw money, and, going online to check their account balance. Such habits have been transformed by internet where everything is dealt with online, including payments and money transfers.

One of the most important examples of innovation in banking is the cross-functionality and the different ways in which to service banks' clients as well as the real-time transactions initiated by all available channels.

In many countries Peer-to-Peer (P2P), as well as instant payment solutions, are flourishing. For example, in some countries banks invested in a new real-time system and developed a shared application for Peer-to-Peer transfer or have started using video channels for client on-boarding and advising customers.

Digitalisation of banks is translated by a transformation from a multichannel approach (focusing on maximising the performance of each physical channel, phone, web, mobile) to an omnichannel approach, putting customer at the centre and promoting the use of channels simultaneously (instead of focusing on corporate silos). All the channels are now linked to one platform with integrated devices, providing a seamless banking experience for customers.



### New Peer-to-Peer payment apps

With new Peer-to-Peer payment apps proposed by banks it becomes easier to pay back someone, reimburse him/her for a restaurant bill, contribute to a collective present for a colleague/friend without sharing your bank details.



### Mobile-Point-of-Sale solution

Several banks have launched a mobile-Point-of-Sale solution, known as mPoS, which allows businesses and self-employed professionals to accept card payments using a smartphone. Other banks have built online communities of merchants using a PoS terminal which allows cardholders to access offers and promotions using geolocation technology.

Transactions and data are updated in real time: world banks offer their clients the possibility to initiate transactions, from anywhere in the world, which banks execute seconds after the client's request has been made. Customers can access the latest information, whatever the channel chosen, and in a single click a customer can access all the accounts he/she holds in a bank. These facilities improve customer satisfaction and – over time – loyalty.

### ■ New designed branches

Modern branches called 'stores' have been designed with equipped self-service areas, with tablets and new digital technologies but also with private areas to provide immediate personalised advice to customers who request it. They are using video channels for client on-boarding and advising customers. Sometimes banks access customers by means of a pop-up store that can be flexibly set up in shopping centres, markets, or remote places. Banking instruments are adapted with digital signage, intelligent ATMs, et cetera. All processes are digitalised, internally, as well as externally.

Benefiting from face-to face access to an experienced banker who knows the customer's specific situation and provides financial advice for all the important financial decisions the customer takes, is key. Branches appear today more as a "meeting place" to complement online banking and services. In this way, technology supports the "branch of the future" and helps to have a closer relationship with the customer. Despite the enthusiasm for new technologies, customers still value a human contact and a physical point of contact for financial decisions or when they face problems. This direct access clearly represents a value for customers when compared to technology companies which are often limited to providing only a switchboard number.



#### **Biometrics ATM solutions**

Advanced biometric solutions have been implemented by banks for ATMs in certain countries. This allows a client to withdraw money without any card. The authentication is made with the client's fingers (or the network of human veins in the fingers) and the PIN code. Biometrics represent a key instrument for certain people with disabilities.



#### **High definition video conferencing to complete mortgage applications**

Some banks have put in place a high definition video conferencing system in their branch to complete mortgage applications in case the staff member who usually handles such applications is not available.

#### **Faster loan application process**

Some banks also created apps which display the unsecured limits for their customers, providing information on how much money they can borrow, and giving them a new way to process a loan application.

## ■ Partnerships with FinTech Companies and start-ups

To succeed in this highly competitive banking landscape, far from being defensive, banks are implementing collaborative strategies with new companies. Certain banks have already made the choice to invest in Financial Technology companies, known as FinTechs, and/or start-ups.

Banks have been involved in buy-outs offering exit possibilities for investors in FinTechs. Banks are also hiring digital innovators and providing funding. Research and development remain key areas for future projects. For some, the banking industry is under threat from the technology industry such as big internet companies and emerging start-ups. But the reality is other: banks work hand-in-hand with technology firms. By becoming closer to technologists, banks ensure that customers acquire the next banking technology solution as quickly as possible. However, the transformation of bank business models requires not only hiring new IT talents but also changing the culture and the approach of the top management.

*“FinTech is a new market. It is 21<sup>st</sup> century finance. It is the new form of banking, and is related but very different to the old form. Some of the old form players will metamorphose into these new digital fintech players. Some, not all. Some of the new players will take over the markets of the old incumbents. Some, not all”*

Chris Skinner

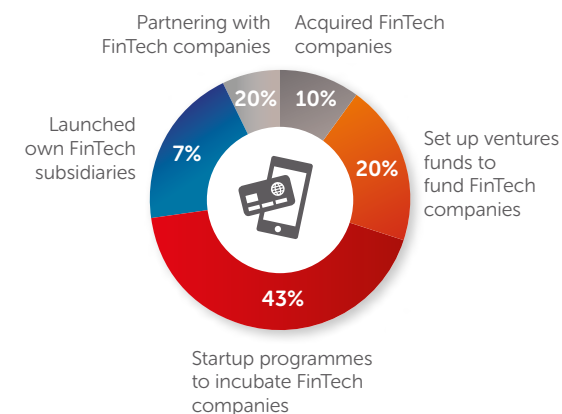
INDEPENDENT COMMENTATOR ON THE FINANCIAL MARKETS THROUGH THE FINANSER AND CHAIR OF  
THE EUROPEAN NETWORKING FORUM THE FINANCIAL SERVICES CLUB



### What does FinTech mean?

“Fintech” are defined as financial technology companies using software to provide financial services, generally presented as start-ups

### How are banks reacting to FinTech?



Source: [thefinanser.co.uk](http://thefinanser.co.uk)

## Digital banking – A strategic priority

The key functions of banks, such as lending, deposits or distribution of currency, will continue to be part of the bank business model. However, this traditional role is by no means sufficient for banks to remain competitive. The role of banks should not be limited to responding to customer demand and providing a secure infrastructure. The role should go further and anticipate customer expectations and next move. Retail banks must offer a broader value proposition to customers. Without changing their approach, traditional retail banks run the risk of becoming obsolete or being pushed back into a back office role, in particular, when considering potentially disruptive technologies (e.g. 'blockchain' technologies), a public ledger of digital transactions using crypto-technology) or forthcoming alternative innovative solutions, launched by new competitors. Importantly, it should be noted that digital players – other than banks - have a different approach towards innovation or digital technology.

These players mostly make money by monetising the data they collect when banks aim at pricing the products they propose. What is more, these new digital companies introduce their products which have a disruptive effect and no regard for regulatory implications. The result being that policy makers have to adapt regulation subsequently (e.g. Uber). This approach necessarily facilitates the emergence of innovative products. Banks generally adopt a different approach. For example, they begin by analysing the compliance regulatory framework and how to adapt their infrastructure accordingly. Banks also invest their resources in implementing prudential regulations which might affect their capacity to innovate.

Consequently, banks appear to face regulatory barriers limiting their innovative ambition, whereas new entrants on to the market seem not to experience the same restrictions.

As the digital future draws closer, the market requires banks to become more network and client-focused. Banks are definitely well placed to take up this challenge, going beyond the financial services they now offer and potentially providing an array of new services. While the competition with new entrants is there, this digitalisation creates new opportunities to engage with customers in a different way. They will become the trusted partner that orchestrates a digital ecosystem around their customers. The change is on-going.

## Cybersecurity – An essential component

Financial institutions are one of the primary targets for cyberattacks. As a result, the industry is committing considerable amounts of money towards protective measures for customers and to maintaining trust.

After a wave of increasingly sophisticated cyberattacks in 2014, targeting all types of organisations, the banking sector is facing attackers which are streamlining and upgrading their techniques rapidly while the sector is trying to fight back at the same speed. These repeated attacks can affect customers' finance, their confidence and have a severe economic and reputational consequences on the organisation. According to the 2015 Internet Security Threat Report (Symantec)<sup>1</sup>, 60% of all targeted attacks last year affected small and medium-sized organisations (SMEs). This creates even greater risks as the majority of SMEs have neither the human nor technological capacity to protect themselves adequately.

Banks in Europe and worldwide are taking these threats seriously. Banks invest heavily in IT systems aiming at the highest possible security levels, but cybercriminals exploit any vulnerability – including on the clients' side to penetrate the system. In addition dedicated regional and global groups have been created, to share information about security threats, for instance, the EU-Financial Services Information Sharing and Analysis Center (EU FS ISAC), and FS-ISAC (global), to share information on security threats. Importantly, awareness campaigns for employees are organised as numerous detrimental activities begin with an email arriving in a bank employee's inbox with a malicious code.

This is also the reason why **the EBF has signed a Memorandum of Understanding in September 2014 with Europol** (and more specifically the European Computer Crime Centre (EC3)). This partnership allows for the sharing of relevant information on cyber threats, as well as targeted actions against specific attacks. The EBF also benefits from the Europol EC3's intelligence which publishes alerts to inform banks, on a continual basis, on cyberattacks and modus operandi.

***“There is and will be no efficient and prosperous European Digital Single Market without digital security and trust. European citizens and businesses have to know and trust that the systems underpinning digital services are safe and secure. Therefore, I have made sure that cybersecurity – which is the very foundation to trust in online services – is one of the strategy's key pillars and top priorities.”***

Günther H. Oettinger,  
COMMISSIONER FOR DIGITAL ECONOMY &  
SOCIETY, EUROPEAN COMMISSION  
SPEECH CYBERSECURITY STRATEGY 28 MAY  
2015.

<sup>1</sup> [Internet security threat report April 2015 – Symantec, Vol.20](#)



## The necessity to adopt a holistic approach

Existing and future regulations will set the framework for what services banks can offer and what competition they will face. If the European Union's top priority is to strengthen its competitiveness and to stimulate investment for the purpose of growth and job creation, it is imperative to link the Commission's digital agenda to the aforementioned goals and that of the Capital Markets Union (CMU) and the forthcoming Green Paper on Retail Financial products and services. Faced with an unprecedented industrial transformation towards a digital future, a more holistic approach is vital. All European Commission services, as well as the other EU institutions should, with the private sector, conduct an assessment on the challenges the EU needs to meet.

Consequently, the impact of any regulation will need to be tested on the (financial) stability, growth and competitiveness of Europe (vis-à-vis the rest of the world). Another focal point for lawmakers is to adopt regulation which embraces the new digital reality. Thus, challenges need to be clearly understood and objectives set accordingly. This is particularly the case in a rapidly evolving digital world. Given the European banking sector's central role in the EU economy, it needs to stand ready to play its part in this wide-ranging transformation.

# EBF key messages

## A successful Digital Single Market with banks

Creating a Digital Single Market (DSM)<sup>2</sup> is one of the ten priorities set out by the President of the European Commission, Jean-Claude Juncker. When Vice-President Andris Ansip presented the DSM strategy in May 2015, he underlined the importance of making the European Union's single market fit for the digital age. According to the European Commission, a properly functioning digital single market could contribute €415 billion a year to the EU economy and create some 3.8 million jobs. Achieving it means tearing down regulatory walls and moving from 28 national markets to a single one.

Creating a Digital Single Market that responds to the reality of the banking market is one of the priorities of the European Banking Federation, which is actively committed to the future of banks.

### ■ What is needed to achieve a successful Digital Single Market?

1. **Banks represent strategic digital partners for Europe's economy. Making Europe "digital" involves banks too.** Banks channel savings to investments to ensure economic activity and growth and provide essential services in a secure and reliable way for their customers, consumers and corporates alike. They embrace the digital innovation opportunity, accelerating the rethinking of their traditional business model, proposing innovative products/apps, engaging in FinTech partnerships, and financing innovative start-ups. Banks perform indispensable functions within the economy and in this way strengthen EU competitiveness and stimulate investment for growth and job creation.

*"By creating a connected digital single market, we can generate up to EUR 250 billion of additional growth in Europe in the course of the mandate of the next Commission, thereby creating hundreds of thousands of new jobs, notably for younger job-seekers, and a vibrant knowledge-based society.*

*To achieve this, I intend to take, within the first six months of my mandate, ambitious legislative steps towards a connected digital single market, notably by swiftly concluding negotiations on common European data protection rules; by adding more ambition to the ongoing reform of our telecoms rules; by modernising copyright rules in the light of the digital revolution and changed consumer behaviour; and by modernising and simplifying consumer rules for online and digital purchases. This should go hand-in-hand with efforts to boost digital skills and learning across society and to facilitate the creation of innovative start-ups. Enhancing the use of digital technologies and online services should become a horizontal policy, covering all sectors of the economy and of the public sector."*

Jean-Claude Juncker,  
PRESIDENT OF THE EUROPEAN COMMISSION









<sup>2</sup> [European Commission priority: Digital Single Market "Bringing down barriers to unlock online opportunities", May 2015](#)

2. **Faced with an unprecedented industrial transformation towards a digital future, a more holistic approach is vital.** Banks are keen to see the economic benefits of a truly effective Digital Single Market. This goal warrants further reflection by banks and EU stakeholders on the possible role of digital financial services when it comes to launching a Capital Markets Union, and, in the context of the forthcoming retail financial services consultation. All European Commission services, as well as the other EU institutions should, together with the private sector, conduct an assessment on the challenges the EU needs to meet and ensure the legislation is adjusted to the digital market reality.
3. **The banking sector supports a competitive and innovative EU Digital Single Market which safeguards existing consumer protection, trust and security. In the banks' view, there is not necessarily a conflict between innovation and security.** The key to a successful Digital Single Market is trust. To protect consumers and their data within a new digital economy, companies offering services similar to those of banks, and facing comparable risks, should be subject to appropriate and equivalent rules. This implies the need to find the proper balance between competition, innovation, security, privacy, and consumer protection. It is crucial to create a Digital Single Market that facilitates the development of all European businesses.
4. **Strengthening cooperation and raising the awareness of EU citizens on the growing threats from cybercrime is crucial.** Making digital finance secure and building trust should be a concern for all, including public and private actors.

*"In 2014 only 15% of consumers bought online from other EU countries, while 44% did so domestically and only 5% of businesses sold their products cross-border online. It is clear that we have yet to fully exploit the potential of the Digital Single Market."*

Věra Jourová  
EUROPEAN COMMISSION FOR JUSTICE,  
CONSUMERS AND GENDER EQUALITY

The EBF Blueprint proposes recommendations on which to build a proper framework for a workable Digital Single Market (DSM) in particular on key issues.

-  Better access to banking products and services
-  Data value chain/big data
-  Digital payments (mobile/instant and e-invoicing)
-  Cybersecurity
-  Crypto-technologies
-  E-identification/e-signature
-  Digital skills (competence/talent recruitment and education)
-  Removing regulatory inconsistencies

# Key Recommendations



## Better access to digital banking products and services

- 1 Develop common modern and simplified set of rules for companies and for the benefit of consumers.
- 2 Develop public-private partnerships between banks and public authorities to increase digital inclusion.
- 3 Avoid discrepancies in national taxation, civil law and product specifications defined by national regulations.
- 4 Ensure interoperability at all levels of the financial services' value chain to facilitate for example switching, payments etc.



## Data value chain / big data

- 1 Promote the benefits of data analytics and ensure coherence in their application.
- 2 Ensure a right balance between data protection and data analytics methods.
- 3 Allow a full use of data analytics in the assessment of creditworthiness and fraud prevention.
- 4 Facilitate interoperability and fair access to digital platforms.



## Digital payments

### Mobile & instant payments

- 1 Enable competition and innovation while preserving trust and security.
- 2 Ensure the newly framed legal environment on payments is conducive to customer confidence and stimulating for electronic payments.
- 3 Clarify several issues on the access to customers' accounts and data information by third-party providers via bank's infrastructure.
- 4 Organise a fully-fledged stakeholders' debate on innovative payments for pan-EU solutions with consideration for costs/benefits for all stakeholders.

### E-Invoicing

- 1 Establish guidance to avoid the development of non-interoperable national solutions and services.
- 2 Develop a communication campaign on the benefits of e-invoicing with a strong commitment from public administrations and financial institutions.
- 3 Build an easily accessible and secure service environment which can facilitate the implementation of e-invoicing in the B2C and G2C domain.
- 4 Establish easy-to-use and cheap-to-implement Euro Retail Payment Board's (ERPB) solutions, enabling businesses to reach all payers in the EU.



## Cybersecurity

- 1 Promote an awareness campaign about existing and new threats; making digital finance secure and building trust should be a common goal for public and private actors.
- 2 Create a framework for cybersecurity's monitoring to strengthen preventive measures and to ensure effective and better coordinated responses to cybercrime at EU level.
- 3 Encourage exchange of information via cross-country public-private partnerships and cross-industry platforms.
- 4 Promote coordination among coexistent initiatives and develop a one-stop-shop mechanism for incident notifications.

# Key Recommendations



## **Crypto-technologies**

- 1** Conduct a joint assessment by both governments and industry participants on the opportunities and impact of crypto-technologies.
- 2** Build a comprehensive regulatory approach to help overcome uncertainty for legitimate users.
- 3** Make transactions subject to the same regulatory standards (ref. to Anti-Money Laundering / Anti-Terrorist Financing - AML – ATF).



## **E-identification / E-signature**

- 1** Establish a truly interoperable environment with the recognition of a preferential use of cross-border national eIDs.
- 2** Encourage confidence in e-identification.
- 3** Establish common standards for document authentication and procedure to ease the use of e-signature at domestic and cross-border levels.
- 4** Establish a common bank industry standard to allow the use of eIDAS under SEPA and the future PSD2.



## **Digital skills**

### Competencies / Talent recruitment

- 1** Build a map of skill profiles to understand the strength and weakness of a bank's knowledge environment and the main gaps to fill in.
- 2** Introduce the implementation of a structured change management process.
- 3** Improve job rotation practice, to help incentives for knowledge exchange and to build multi-skill professional profiles (e.g. through structured job rotation).
- 4** Improve employee skills and competencies via training initiatives focusing on the conduct of a digital/ online business to guide customers appropriately.
- 5** Strengthen a collaborative work environment suitable for knowledge exchange and innovation.

### Digital education

- 1** Launch, with the EU and international authorities, initiatives to promote digital financial expertise in society as a whole.
- 2** Improve digital skills and financial literacy among children, starting with school programmes.
- 3** Raise awareness on benefits of digital products and services and cybercrime risks.
- 4** Start partnerships with other interested parties to initiate forward-looking discussion on the benefits of digital financial education.



## **Removing regulatory inconsistencies**

- 1** Conduct a 'fitness check' of existing financial services legislation to adjust to the digital market reality and ensure consistency.
- 2** In the context of the 'fitness check' proposed, create a platform for discussion with the European Commission's DGs to ensure consistencies.
- 3** Ensure the Digital Single Market balances competition and innovation with trust and security.
- 4** Safeguard the right balance between data protection requirements and profiling for fraud prevention and creditworthiness assessment.





## Better access to digital banking products and services

The fast-growing digital society creates many opportunities: for customers who can access various and increasingly seamless banking products and services, and for banks, which improve their understanding of customers' needs and increase their business opportunities. In order to make the access to banking products and services in this online world, a reality, the barriers identified should be removed.



## Opportunities for banks and customers

- Access to banking product and services is constantly increasing. Almost four in five persons - 79% - who use mobile banking in Europe have bought an item using their mobile device in the last 12 months; and more than half of those customers surveyed believe that they will either “certainly or probably” use a mobile payment app in the next 12 months<sup>3</sup>.
- Banks have started to make significant **investments to improve the access of their customers to their new digital banking products and services**. In particular, this implies the development of sophisticated technologies such as biometric, audio, voice and image recognition software, data analytics and high-performance computing infrastructure. Today, banks provide customised deals at select stores through mobile apps, 24 hour, 7 days a week, account balance control, new concept stores or remote adviser systems connecting financial experts to customers from their branch or a mobile device via high quality video which allows financial planning, problem resolution and assistance/advice.
- These new innovative banking solutions let banks provide a **‘tailor-made’ customer experience which facilitates a faster access to banking products and services**. More importantly, they ease the interaction between banks and their customers who are able to search further and faster for the best deals/value when and how it suits them. Now instead of having numerous passwords or log-ins, a number of banks propose biometric security solutions to customers, such as facial, fingerprint or voice recognition tools. The contact customers have with a bank also goes through new channels such as social media (e.g. Twitter, Facebook) or secure instant messaging platforms similar to Viber or WhatsApp.
- New banking technology also has a **positive impact on the management of customer finance**, especially via budgeting programmes developed by banks or through automated advice. It further contributes to helping consumers avoid financial mistakes such as overlooking the payment of bills and running into overdraft. This potentially prevents customers from being charged penalty fees. According to a recent survey<sup>4</sup>, the vast majority of people who use mobile banking indicate their money management has improved since the use of technology. For example, they feel more in control of their finances, do not miss payments and save more. In fact, 85% of mobile bank users in Europe indicate at least one way their money management has improved since they began using a mobile bank. In some countries, such as Italy, Romania or Poland this is 90% or higher.

<sup>3</sup> The ING International Survey on Mobile Banking, New Technologies and Financial Behaviour 2015: The ING International Survey of 14,829 people was conducted by Ipsos using internet-based polling. Fifteen countries were surveyed overall: Austria, Belgium, Czech Republic, France, Germany, Italy, Luxembourg, the Netherlands, Poland, Romania, Spain, Turkey and the United Kingdom (13 European nations) and respondents from the USA and Australia. Polling took place between 16 January and 2 February 2015.

<sup>4</sup> See footnote 3

### Improvement of the money management

**85% of mobile bank users in Europe indicate at least one way their money management has improved since they began using a mobile bank.**

In some countries, such as Italy, Romania or Poland this is 90% or higher.



Source: The ING International Survey on Mobile Banking, New Technologies and Financial Behaviour 2015.

### Fast access without any codes

Instead of having numerous passwords or log-ins, some banks propose biometric security solutions to customers, such as facial, fingerprint or voice recognition tools.

With a thumb print on the screen he/she has direct access. It saves time and removes the need to remember passwords digit codes.

- Through the development of analytics tools and algorithms, banks will be able to anticipate proactively the best time to provide advice to the customer without waiting for him/her to come to a branch. As a result, the advice is likely to have a more effective impact on the financial decisions taken by the customer during his/her lifetime. In this way customers can prepare key events more effectively (e.g. having a child, getting married, buying a house, travelling). Logically, online and personal advice will become complementary tools in the future.
- Digital technologies will also **improve financial inclusion** in reducing, for example, geographical distances and reaching customers located in peripheral areas to allow them to benefit from more offers.
- **Banks as universal players are committed to serving all customers.** Some customers do not like change and prefer things to 'stay the same'. For instance, most banks actively support elderly people and non-digital clients who find it difficult to embrace new digital banking services. This might not be the case for new entrants on to the market. Banks achieve this by putting in place tools appropriately adapted. For instance, trained employees providing free advice (from how to shop online to protecting privacy) and digital financial education programmes.

*“Consumers and companies in Europe are digitally grounded. They cannot choose or move freely. In the 21<sup>st</sup> century, this is absurd.”*

Andrus Ansip  
VICE- PRESIDENT DIGITAL SINGLE MARKET,  
EUROPEAN COMMISSION

## Barriers to (cross-border) digital access /e-commerce

Well-known obstacles to the provision of product and services within the single market remain the same at cross-border level. Furthermore, it is paramount to keep in mind that selling financial products or services has potential risks and financial consequences quite distinct from those associated with selling books or shoes.

- **Culture/language barriers** create numerous difficulties at every step of the purchasing process on internet as the information is usually only available in the language of the country in which the product or service is sold. For instance, the information provided on websites at the pre-contractual, contractual phase, and post-contractual phase regarding the after-sale service, though in some cases banks try to make information available in English. Not surprisingly, history, tradition and culture necessarily influence the design of the products and services which are adapted to specific customers needs; needs which differs from one Member State to another.
- **Different national consumer protection and contractual laws across the 28 Member States.** As expressly stressed in the Digital Single Market Communication, one of the reasons why consumers and companies do not engage more in cross-border e-commerce is because the national consumer protection and contract laws differ throughout the 28 Member States and companies need to act in most of the cases in accordance with the host countries' national consumer protection laws and supervisory measures. This is also true for the retail financial services markets, still very fragmented. This is mainly owing to the different consumer/investor protection rules, despite the EU initiatives on consumer & mortgage credit or payment accounts.

Despite banks' willingness to develop cross-border activities, they have had to invest huge amounts to ensure they comply with the national legislation on a daily basis (especially as national legislation is subject to regular review). In this instance, the resources invested for compliance purposes are not invested in the development of innovative solutions. This situation prevents consumers from benefitting from the most competitive and innovative online offers.

- **Discrepancies in national taxation, civil law and product specifications defined by national regulations:** the progressive integration led by the EU to date does not fully include tax systems and civil law in every Member State. The difficulties of having to deal with many different national systems when trying to offer services cross-border both on and offline constitutes a tangible obstacle for companies, including banks. Diverse national tax regimes prevent banks from designing pan-European retail products, and diverging national civil law regimes require providers to adapt product strategies locally.
- Access to financial services will increase via automated financial services, allowing customers to make choices faster and take their own decisions. However, here, clarification needs to be brought to the issue of liability.
- **Access to customers' accounts and data information by third-party payments providers via banks' infrastructure.** The new Payment Services Directive (PSD2) stipulates that the "account servicing payment service providers" (namely banks) shall make possible for "payment initiation service providers" (third-party payment providers) to rely on the authentication procedures provided by banks to initiate a specific payment on behalf of the payer. It means that third-party payment providers will have access to clients' accounts and customer data information via the banks' infrastructure. The challenge is to ensure security and privacy for both banks and consumers in this new scenario. Indeed, the structure behind the functioning of certain payment initiation services/third-party payment providers potentially calls into question the banks' measures to keep online banking secure, and per se, might put at risk existing anti-money laundering and fraud prevention measures already in place. A clear liability framework, as well as appropriate technical standards, should be implemented to face fraud incidents and data protection. (See EBF Blueprint chapter on Digital Payments and Removing regulatory inconsistencies).
- **Interoperability is also required at the level of the bank, the switch, and the payment channel.** Sometimes new technical services occur in a "walled garden" because interoperability is not technically allowed. Consumers wishing to swap between apps services must have multiple solutions and will not be able to switch between different digital wallets or services (incurring time, effort, and extra fees). In short, digital inclusion and interoperability is essential in order to avoid financial or social exclusion.

## RECOMMENDATIONS

### Better Access

- 1 Develop a common, modern, and simplified set of rules for companies and the benefit of consumers.** A common, modern and simplified set of rules to sell online and across borders, should be updated based, on the Consumer Rights Directive, the General Data Protection Regulation and the e-Privacy Directive. The rules should take into account the particularities of the financial services' products and services which differ from the usual retail products. A new framework should not jeopardise incentives to innovate as banks are instrumental players in driving innovative solutions. The forthcoming retail green paper on financial services should help in this respect.
- 2 Develop public-private partnership between banks and public authorities to increase digital inclusion via education programmes etc.**
- 3 Avoid discrepancies in national taxation, civil law and product specifications defined by national regulations.**
- 4 Interoperability should be ensured at all levels of the financial services' value chain to facilitate, for example, switching and payments.**





## Data value chain / Big data

The use of data is growing exponentially, in terms of use, variety, volume and velocity. Data are at the centre of this digital revolution and consequently the use of data analytics is creating increasingly new opportunities both for consumers, who can benefit from more innovative and tailored products and services adapted to their needs, and for companies able to develop new businesses.

“Data analytics” more commonly called “big data” describe the volumes of data provided by consumers, generated by different business activities and customer behaviour, as well as data collected from new sources such as the social media. Some of these are personal data. If so, they are usually aggregated anonymously or pseudo-anonymised or based on informed consumer consent. Data analytics contribute widely to a better internal understanding of the bank’s activities, a more effective risk management, and an improved monitoring of compliance. They can also contribute to building a stimulating customer experience. This said, banks still face a number of challenges in the technical implementation of data analytics.





## Opportunities for banks and customers

- **The use of data analytics has many advantages from a customer experience point of view:** the data collected, based on customer's informed consent (when required) will improve the understanding of customer's needs, the quality of products and services and facilitate the development of personalised offers in real time. Consumers will, for instance, be able to benefit from more flexible offers for loan rates' or a simplified and faster approval of their loan's request due to a better assessment of the risk profile. Data analytics also offer opportunities to identify potential warning signs in terms of fraud or creditworthiness assessment. Thus, data analytics will create personalised offers for customers and avoid over-marketing of products not needed.  
  
Given the changes in society and the use of social media, the new generations of customers arrive with fresh expectations. They expect banks to take into account the data, already at their disposal, when offering services. Customers are increasingly willing to accept the sharing of data and are inclined to forego privacy either in exchange for more tailor-made products and services, 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. Data analytics, generally, contribute positively to maintaining trust, transparency and security.
- Banks have a longstanding expertise in dealing with trust, confidentiality and IT security. This ability potentially distinguishes the bank in the services it offers from the new entrants on to the market. Trust in banking services remains a priority for all consumers who seek, at the same time, to take full advantage of the opportunities offered by the new banking environment. Data analytics can contribute positively to maintaining trust, transparency and security.
- The use of Big Data in the banking sector is also attractive from a business point of view: it will develop the performance of banks, banking techniques, such as credit analysis, and create new business opportunities. Data analytics constitute a key tool to understanding a bank's business and activities more thoroughly. It also contributes to more efficient risk management and compliance. For instance, the tool can be used to monitor and develop financial performances and the risk profile of banks. The use of data analytics represents a competitive advantage that allows banks to run their business more efficiently and at a lower cost. Data analytics will enable banks to adapt to new digital consumer expectations and thus reduce inappropriate marketing expenditure, avoid the development of unnecessary product and services offerings, and focus more effectively on their capacity to innovate for the good of society and its stakeholders.



### What is big data analytics?

Big data analytics is the process of examining large data sets containing a variety of data types ('Big Data') to uncover hidden patterns, unknown correlations, market trends, customer preferences and other useful business information. The analytical findings can lead to better customer service, improved operational efficiency, more effective marketing, new revenue opportunities, competitive advantages over rival organisations and other business benefits.

Source: Techtarget - Essential Guide

## Barriers to the benefit of data analytics

- **Data ownership:** it might be difficult to identify the legal owner of the data collected as this could depend on where the data comes from, how it is archived, and whether it is linked to intellectual property rights or data protection requirements. It should be noted that **big data has no value in itself**, it is the algorithm and analytic ability of the bank which produces the end value. Consequently, it depends on the cost and time invested in the collection, organisation and accessibility of the data, as well as the necessary IT infrastructure and cloud-based technologies needed to store, process and analyse it. What is more, the customer who gives his/her informed consent, has the right to access, delete or modify the content of the data stored by the data processor. **The EBF underlines the necessity for a common data standard to be shared by all European financial services providers.**
- **Cloud computing challenges:** the financial industry is still in the early stages of cloud adoption due to specific important concerns over security. For the banking sector, public breach notification, security incident, data security, malware and hacking are considered critical risks to be avoided. Uncertainty regarding liability issues also need to be clarified. To be noted too, are the requirements imposed by financial industry regulators with regard to outsourcing e.g. cloud computing for audit. Likewise, the international dimension of cloud computing should be taken into account. We observe a lack of level playing field in the storage of data via cloud computing: EU players face certain geolocalisation and data privacy restrictions whereas US players do not and are able to use data stored on the cloud all over the world.
- **Pseudo-anonymisation or anonymisation of personal data** for analytics or processing in cloud computing is more costly, time consuming and complex as data must be pseudo anonymised in the private cloud of the bank's data center, then uploaded to the public cloud for processing and finally downloaded back to the private cloud for reidentification of the personal data to analyse and propose the necessary services or products. Personal data of European customers have to be geolocalised in European territory. This creates extra burdens and costs to European companies in comparison to players outside Europe that don't have to comply with the same rules (EU Data Protection Regulation) and hence an unlevel playing field.



### What is Pseudo-anonymisation?

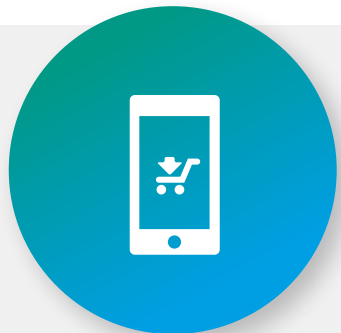
"Pseudo-anonymisation" is usually used in the context of profiling and consists in replacing the "most identifying" data by a unique number or name to ensure the data record is "less identifying", to avoid potential concerns regarding data sharing and data retention. This process is different from "anonymisation" as the latter will not allow a reverse compilation. It can irreversibly prevent identification of the data subject.

- To be noted, are the ongoing discussions on the proposal for an EU Data Protection Regulation on a possible restrictive definition of profiling which may limit considerably the possibilities for banks to know their customers better, to conduct creditworthiness assessment, and to prevent fraud. A clear standard that makes the user consent process more transparent, quick and easy for user profiling and analytics, should be supported.
- **Employees with the right skills and competencies:** “handling” and “processing” data rely on innovative solutions involving technological, analytical and interpretation of the data. This requires highly qualified employees (data strategists, engineers, statisticians, data analysts etc.) who need to develop specific analytical skills to deal with complex big data management systems.
- **Lack of harmonisation among supervisors:** it is difficult for banks to benefit fully from the data analytics opportunities as they are subject to specific supervision, whereas businesses not falling under the supervision of financial regulators possess their client’s financial data (e.g. social networks). The European Central Bank has not yet clarified the rules for the use of data analytics by supervised banks and we observe that some national regulators appear to be more liberal than others. Furthermore, there seems to be divergent expectations as to how banks need to deal with data security and data breaches. Hence, a sectoral harmonisation should be favoured.
- **Legacy of banks’ IT systems’ infrastructure:** the growing volume, variety and velocity of data needs to be connected throughout organisations and departments in order to give “ready access” to products and customer information. Some banks may still be working on partly decentralised or fragmented systems. It is important to ensure that banks take full advantage of their infrastructure to share and benefit from internal data across their organisation. Thus, banks should adapt their IT systems according to the expectations of data-driven customers.

## RECOMMENDATIONS

### Data value chain / big data

- 1 **Facilitate interoperability and fair access to digital platforms.**
- 2 **Promote the benefits of data analytics and ensure a coherence in their application.**
- 3 **Ensure the right balance between data protection and data analytics methods to allow balanced restrictions on profiling (e.g. preserve informed consent but make this provision more flexible for fraud prevention/detection or creditworthiness assessment); allow personalised and anonymised data; and link data ownership to the data analytics capabilities of the company.**
- 4 **Allow the full use of data analytics in the assessment of creditworthiness and fraud prevention.**



## Digital payments

### Mobile & instant payments

Payments were notably the first banking services to go digital (online and/or mobile) with the verification of the bank account balance being the most frequently used, and opening the door to new phases of digital banking. The digital customer expects payments to be seamless and mobile, and wants to be able to buy products and services whenever they want from wherever they are. All processes, infrastructures, systems, rules initially designed for “traditional” paper-based payments are currently being adapted/modified/created to cater for the new nature of payments.

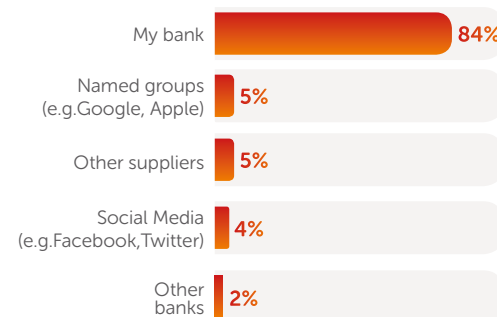


## Opportunities for banks and customers

- European banks offer new and innovative banking products to their customers in an environment where new technologies strongly stimulate innovation in payments. They have the potential to retain a key place in the payment chain, via their infrastructure and through the mix-innovative payment solutions they offer and – in addition – smart solutions offered in partnership with other providers such as financial technology companies (Fintech).
- Mobile and digital payments will offer the possibility to streamline many processes which are traditionally paper-based or manual via Digital Channel Service Interface, contactless payment systems and mobile wallets. This will be more and more the case with instant or real-time payments and real-time Peer-to-Peer payments allowing immediate transfers of money to another person. i.e. payments will be immediate, 24 hours a day, each day of the year.
- This will certainly help to meet customer demand and expectations including – but not limited to – the uptake of e-commerce and m-commerce services.
- Banks in Europe have developed a second-to-none payment infrastructure which is highly efficient, secure and reliable. Every day more than 400 million retail payments are processed without error in Europe. Maintaining and improving this infrastructure is costly and requires a sustainable business model.
- The Single Euro Payment Area (SEPA) makes all retail electronic payments in the euro area as easy as euro cash payments, providing fast and secure transfers between bank accounts anywhere in the eurozone, facilitating cross-border payment with the use of credit transfer, direct debit and payment card, ensuring transparent pricing and a foolproof guarantee that a payment has been received for its full amount. SEPA will also become a reality for euro-denominated payment in non-euro area countries from 31 October 2016. Banks are now busy adapting the infrastructure and systems to instant, digital payments, and providing integrated services across all payment channels and instruments.
- The use of cash may be reduced as well as any related management costs.

### Preferred for mobile payments

Most respondents in a 2015 ING survey said they prefer their own bank over other online services when conducting mobile payments:





## Barriers to consumer protection and security

- The challenge of new entrants and new models adds a new dimension to the changing role of banking. New entrants are establishing digital-only banking models, and established players in other sectors continue to develop products and services to challenge the incumbents. **However banks' infrastructure safely connecting the accounts of all customers will continue to be the backbone of the universal payment system.**
- Banks recognise the need to change business models, to update systems, and processes. Nonetheless, a **truly level playing field should be guaranteed** to ensure that similar rules apply to all payment services providers. Those rules should remain the same regardless of the type of institution.
- The recently reviewed Payment Services Directive (PSD 2) stipulates that the "account servicing payment service providers" (namely banks) shall make it possible for "payment initiation service providers" (third-party payment providers) to rely on the authentication procedures provided by banks to initiate a specific payment on behalf of the payer. This means that third-party payment providers will have access to client accounts and customer data information via the banks' infrastructure. The challenge is to ensure security and privacy for both banks and consumers in such a new scenario. Indeed, the structure behind the functioning of certain payment initiation services/third-party payment providers potentially calls into question the banks' measures to keep online banking secure, and per se, might put at risk existing anti-money laundering and fraud prevention measures already in place. A clear liability framework, as well as appropriate technical standards, should be put in place to face fraud incidents and handle data protection. (See *EBF Blueprint chapter on Better access and Removing regulatory inconsistencies*).
- Digital banking services require a high level of security to protect against the risk of fraud, theft and misappropriation of data. The right framework should be put in place to guarantee a correct level of data protection and security at EU level.

## RECOMMENDATIONS

### Mobile & instant payments

- 1 Enable competition and innovation while preserving trust and security.**
- 2 Implement the newly framed legal environment on payments - Interchange Fees Regulation and Payment Services Directive 2 (PSD2) - in an efficient and forward-looking manner, conducive to customer confidence and stimulating for electronic payments. Monitor closely the potential fraud, privacy and data protection incidents which may arise.**
- 3 Clarify several issues of the access to customer's accounts and data information by third-party providers via banks' infrastructure: the liability framework, the authentication methods and the customer's data which TPPs are allowed to retrieve.**
- 4 Organise a fully-fledged stakeholders' debate on innovative payments for pan-EU solutions with costs/benefits consideration for all stakeholders involved.**
- 5 Continue the dialogue with EU policy makers and supervisors with an open and constructive approach as regards the other suppliers who play an increasing role in digital services.**
- 6 Develop banks' potential role in e-identity via Electronic identification and trust services (eIDAS).**

## E-invoicing

E-invoicing per se is not directly a payment matter. It is a commercial or business matter between two counterparties in a sales transaction: the seller and the buyer. This said, the European standard on e-invoicing (as required by Directive 2014/55/EU) will be, together with the Single European Payment Area instrument, one fundamental building block to enable the development of fully automatic e-invoicing and payment solutions at the pan-European level.

A wide adoption of e-invoicing is expected to spread benefits in both efficiency and cost savings. In Europe, according to a research issued by Billentis<sup>5</sup>, the annual invoice volume is expected to reach €35 billion. Already, in 2015, the general expected volume of e-invoices is totalling €7,5 billion. The biggest incentive for accelerating the general diffusion of e-invoicing processes is represented by the potential cost savings. It is important to highlight the presence of Electronic Bill Presentment & Payment (EBPP) solutions that are managed either directly or indirectly via Payment Services Providers and can be used in the Business to Customer (B2C)/Government to Customer (G2C) and Business to Business (B2B) domains. For consumers, it means handling invoice payments faster and more easily and for business companies it increases efficiency throughout the payment as well as the overall reconciliation process.

5 [E-Invoicing / E-Billing International Market Overview & Forecast, February 2015](#)



## Opportunities for banks, customers and billers

- At both national and international levels, the success is growing for services that allow a company or a governmental agency to send virtual bills to their clients. This enables the automatic payment through Internet - Electronic Bill Presentment and Payment (EBPP) - and simplifies the accounting reconciliation processes of these services for the bills' issuer. Besides the companies which provide EBPP "Biller Direct" services, the banking industry, in the role of Banker Aggregator, has achieved new EBPP solutions that allow the consumer to make, on a bank's website, payments to multiple billers that are pre-registered to receive payments.
- In addition, the banking sector is providing services for e-billing in a multichannel logic that allows payments through several channels such as Home/Corporate banking, ATMs and mobile phones, and a multibank logic that overcomes the limitations associated with a single bank system. Multichannel and multibank logics are considered the specific success factors for the development and diffusion of such services.
- For consumers, this e-billing solution will create a more satisfactory user experience (easier payments, availability 24/7, etc.), increase high security levels in electronic transactions and ensure availability of successful charge notice and reduced use of papers (electronic storage).
- For billers, it will offer a further extension of the commercial offer for clients and the possibility to reach a higher number of online users, both retail and corporate. E-billing will necessarily improve efficiency as transactions are quicker, more secure and traceable and accounts' reconciliation processes, are simplified. The customisation of services will also offer advantages to suit specific requirements.
- The models, now widely used internationally, involving an active role for the banking community, are mainly based on centralised multibank application platforms, which are often managed by operators already active in payment processing or document management.

More recently, the need to integrate the document exchange process with the payment process has led several companies to enter into agreements with operators having a strong local presence, such as supermarket and tobacconist networks. They also accept other payments, such as credit cards. This model allows the consumer to authorise payments of expense accounts, at any local retail point.

- For the financial institutions, **several opportunities could arise from this specific process** including increased efficiency and reduced overall costs, decreased use of paper (electronic storage) and relative paperwork management. It also offers a higher level of traceability, process control and internal storage (due to the digital form of the data). In terms of security, e-billing will offer better collateral services because of their integration with security tools (digital signature, encryption, end-to-end, etc.). In general, e-invoicing with shorter payment delays will lead to fewer errors as well as reduced printing and postage costs. What is more, it will have a positive impact on the environment and energy consumption.

## Barriers to e-invoicing implementation

The 2014/55/EU Directive has made e-invoicing in public procurement mandatory by 2016 and now calls for a European standard related to the semantic data model of elements at the core of electronic invoices. This said, the take-up of e-invoicing and related payment solutions in the EU is at an early stage and several barriers have been identified by the Euro Retail Payment Board (ERPB):

- Businesses and consumers have a limited knowledge of the advantages and added value owing to lack of motivation to initiate change.
- SMEs and micro-enterprises perceive e-invoicing/billing and the integrated presentment & payment solutions as complex and expensive to implement.
- Consumers lack access to comfortable and secure solutions for receiving and paying e-invoices/bills.
- The payers (and even the payees) might experience a lock-in effect because of divergent service levels and complexity in switching.

## RECOMMENDATIONS

### E-invoicing

- 1 Establish guidance for the market actors to avoid the development of non-interoperable national solutions and services.**
- 2 A communication campaign should be launched on the benefits of e-invoicing with a strong commitment from public administrations and financial institutions.**
- 3 Give a leading role to public authorities which could take a leading role in promoting e-invoicing by showing the example.**
- 4 Build an easily accessible and secure service environment which can facilitate the implementation of e-invoicing in the B2C and G2C domain.**
- 5 Establish easy-to-use and cheap-to-implement Euro Retail Payment Board (ERPB)P solutions, enabling businesses to reach all payers in the European Union.**



## Cybersecurity

With a shift in activities from the more traditional IT supports to mobile applications with instant/contactless payments, the criminal activities are shifting as well. **One constant in cybercrime is change.**

According to the European Commission's Special Eurobarometer 423 on Cyber security<sup>6</sup> (February 2015): "Internet users in the EU remain very concerned about cybercrime. When asked how concerned they are about experiencing or being a victim of different types of cybercrime, Internet users are most likely to say they are concerned about identity theft (68%) and discovering malicious software on their device (66%). Internet users also express concern about being the victim of bank card or online banking fraud (63%)". The Symantec report<sup>7</sup> of 2015 mentions that targeting the real names, the ID numbers, the home addresses, the financial information and finally the date of birth are among the top five data breaches identified in the number of incidents in 2014.

The EU institutions broadly recognise cybersecurity as a key priority within the European Agenda for Security<sup>8</sup> or within the Single Supervisory Mechanism<sup>9</sup>. Securing the data of its clients is one of the banks' top priorities. For the banking sector, it is key in order to avoid undermining the confidence of the public in payment systems and infrastructures. Likewise, in the capacity of banks to protect the data of their customers, especially, when consumers have become highly sensitive to privacy issues.

<sup>6</sup> [European Commission's Special Eurobarometer 423 on Cyber security](#)

<sup>7</sup> [Symantec internet security report ISTR20 report April 2015.](#)

<sup>8</sup> [The "European Agenda on Security", published by European Commission on April 28th 2015](#), identify cybersecurity as one of the main three priorities for European security, together with terrorism and serious and organised cross-border crime.

<sup>9</sup> The cybercrime risk has been identified also by the Single Supervisory Mechanism (SSM) as a strategic topic, for its supervisory activity in 2015, and it has to be considered by banks when performing their operational and IT risk assessment.



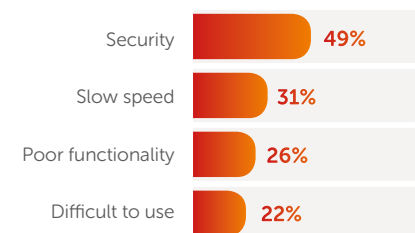


## Opportunities for banks and customers

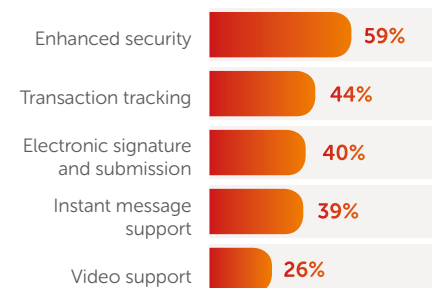
- **Cybersecurity resilience is not something new for the banking sector.** Its strong capacity to be resilient to cyberattacks is essentially based on the fact that banks realised at an early stage that security was fundamental for their customers and essential for delivering secure services. Based on the existing know-how this awareness allows the banking sector to increase trust among customers in the new innovative digital services it offers.
- **The banking sector benefits from an important infrastructure enabling a flow of secured information on the possible threats.** Given this efficient infrastructure, banks can put in place appropriate countermeasures, and consequently, are well placed to secure the interest of their customers in the face of the global cybercrime phenomenon.
- **The European Banking Federation believes in the success of public–private partnerships to fight cybercrime and to prosecute perpetrators.** In 2014, it signed a Memorandum of understanding (MoU) with Europol (EC3). In this agreement, both organisations exchange information and work on awareness of specific threats to the sector.

### Security as top concern

What do customers see as the main concerns when using digital channels?



What do customers want from their bank?



Source: [Ernst & Young Survey, 2014](#)

## Barriers to a successful cybersecurity system

- Criminal modus operandi are becoming more and more sophisticated (phishing techniques and the spread of a multitude of banking malware variations/ permutations). In 2013 a record number of breached data cases occurred in terms of identities exposed in the sector. **The banking sector needs to adapt fast and continually. This implies costly investments.**
- **Criminals act from countries in which judicial cooperation has traditionally been limited** and consequently it is difficult to track them down or/and gather evidence to arrest them. It is therefore critical to enforce public-private partnerships in order to set-up an operational cooperation able to investigate online frauds and prevent future financial crimes. For this purpose, Europol launched in 2014 a joint cybercrime task force (J-CAT) dedicated to strengthening the fight against online crime across the world. The members share intelligence, align priorities and gather data on specific criminal themes from national repositories to propose targets for investigation. The J-CAT is trying to coordinate international investigations against major threats (with the underground fora and malware, including banking Trojans, among the top targets). Considering the risks, it is imperative to balance the need for privacy and security with new digital services according to the risk appetite.
- The current Data Protection Directive and the future General Data Protection Regulation are restricting direct sharing of Indicators Of Compromises (IOCs) with personal information between banks. The EBF would advocate a **more proactive and efficient way to share incidents between banks**. Organised financial industry fora already exist which share IOCs but could be improved by being allowed to exchange IOCs with personal information. In addition, the EBF would like to see a one-stop-shop mechanism when a notification is requested, as currently banks have to notify several authorities in different countries at the same time. Aggregation of incidents in a single point of contact when they occur in several countries within the EU, and outside, needs to be fast and efficient from the legal point of view.

## RECOMMENDATIONS

### Cybersecurity

- 1 Promote awareness campaign about existing and new threats. Making digital finance secure and building trust should be a common goal involving public and private actors.**
- 2 Enforce public-private partnerships cross-country and cross-industry:** it is fundamental for setting up an operational cooperation to investigate and prevent future financial crimes in order to have a broad view of the phenomenon and to increase the effectiveness of cyber intelligence methods.
- 3 Create a framework for cybersecurity monitoring to strengthen preventive measures and ensure an effective and a better coordinated response to cybercrime at EU level:** the creation and maintenance of specific skills and expertise are essential to elaborate and correlate data correctly, as well as to select and draw out the relevant information on the attacks and the mechanisms used. Similarly, it would be relevant to analyse and report cyberincidents for notification and prevention purposes: changing the view from reporting to early warning through the extraction of key messages and "lessons learned" from information and incident sharing. Cybercriminals work more frequently under international coordination and management, with a well-structured segregation of duties, often spread across several countries.
- 4 Encourage exchange of information via public-private partnerships cross-country and cross-industry platforms**
- 5 Promote coordination among coexistent initiatives and develop a one-stop-shop mechanism for incident notifications.**



## Crypto-technologies

Crypto-technologies are one of the major IT innovations to have appeared in recent years, proposing new systems, processes and ways to transact. They provide a distributed recording system which guarantees the possibility of identifying irrefutably transactional data. Furthermore, they build and monitor any transaction or event via a joint network without intervention from a third party or central authority.



## Opportunities

- **The underlying technology of a distributed ledger, also called “blockchain”, provides a number of interesting opportunities both for financial institutions individually and for the collective ecosystem.** The “blockchain” ledger can link individuals and companies to virtual acquisitions and ownership by allowing individual parties to process payments and verify transactions. More importantly “blockchain” technology offers an extremely high level of security. In the case of asset registry, for example, the use of a public ledger to register asset will limit the intervention of a central authority. Transactions will include a reference to an existing asset, meaning that the ownership of the asset will also be the owner of the private key to the public record.
- Using such technology offers clear opportunities to reduce costs of moving and handling money, to secure consumer spending, and to introduce greater liquidity to the market. It also improves offers of products and services and increases banks’ velocity in all their activities.
- The digital ledger of transactions can be used to enable the digitalisation of components of the current financial system. Its implementation would establish an extensible, decentralised, trustworthy, and immutable generic transaction store that enables encoding of business logic, laws, and other rules. Those new technologies will lead to automated processes and documentary tasks, leading to a reduction of the costs (e.g. in the case of credit record with the use of multi-signature wallet, transactions could be executed automatically).
- Companies are currently developing applications using crypto-technologies’ underlying technical innovations to increase transparency and efficiency, benefitting consumers, merchants, governments and regulators alike.

## Barriers

- Crypto-technologies are still in a building phase due to **the lack of common approach and uniform platform**. For example, when looking at crypto-currency schemes, we have to observe that many of these have not yet achieved the maturity levels that would otherwise be expected from a currency. For example, they do not offer consumers the same level of protection as the currency made legal tender through government decree. "Bitcoin" crypto-currency represents probably one of the most well-known examples of crypto-technology. However, its future as a currency is unclear, given that it was built as an experiment.
- The European Banking Authority (EBA), in an opinion<sup>10</sup> published in 2014, identified more than 70 associated risks of crypto-currency schemes, most of them related to money laundering and other financial crimes. Yet, the same report also demonstrated that with a proper body of regulation, most of those risks could be mitigated. Regulatory initiatives in relation to crypto-currency schemes and participants in the value chain (i.e. such as the Federal Reserve System's (FED) assessment on Crypto-currencies Exchangers to be considered as Money Transmitter) would build trust and improve the strength of those platforms.

The EBA also recommended that EU legislators consider declaring market participants at the direct interface between conventional and virtual currencies (e.g. virtual currency exchanges), to become "obliged entities" under the EU Anti-Money Laundering Directive and thus subject to its anti-money laundering and counter-terrorist financing requirements. Differences between schemes should also be taken into account so as to develop a comprehensive regulatory framework that brings certainty to the technology beyond "crypto-currencies". Application and acceptance by customers is not yet clear. Considering the forthcoming regulatory developments in crypto-technologies, a close monitoring of the evolution of the regulation and a better understanding of the use of this technology is recommended, particularly, in the context of "instant payments" and "inter-PSP payments".

<sup>10</sup> [EBA Opinion on 'virtual currencies', 4 July 2014](#)

## RECOMMENDATIONS

### Crypto-technologies

- 1 Conduct a joint assessment by both governments and industry on the opportunities and impact of crypto-technologies** (ranging from land registry automation to improved Anti-Money Laundering processes, faster clearing and settlement cycles in payments and more automated and electronically auditable services in the financial securities' space). Maintaining innovation should remain however a prerequisite for the development of crypto-technologies.
- 2 Build a comprehensive regulatory approach to crypto-technologies to help overcome uncertainty for legitimate users e.g.** transactions in crypto-currencies should be subject to the same regulatory standards as transactions executed in electronic or physical money, in particular in relation to Anti-Money Laundering and Terrorist-Financing. This would also protect consumers from fraud or high-risk exposure. Consumers and companies using services involving crypto-currencies should benefit from similar levels of protection as conventional payment services' providers in terms of oversight, compliance, consumer protection, governance requirements and information obligations.
- 3 Make transactions subject to the same regulatory standards** (Anti-Money Laundering Financial Action Task Force (AML – ATF))



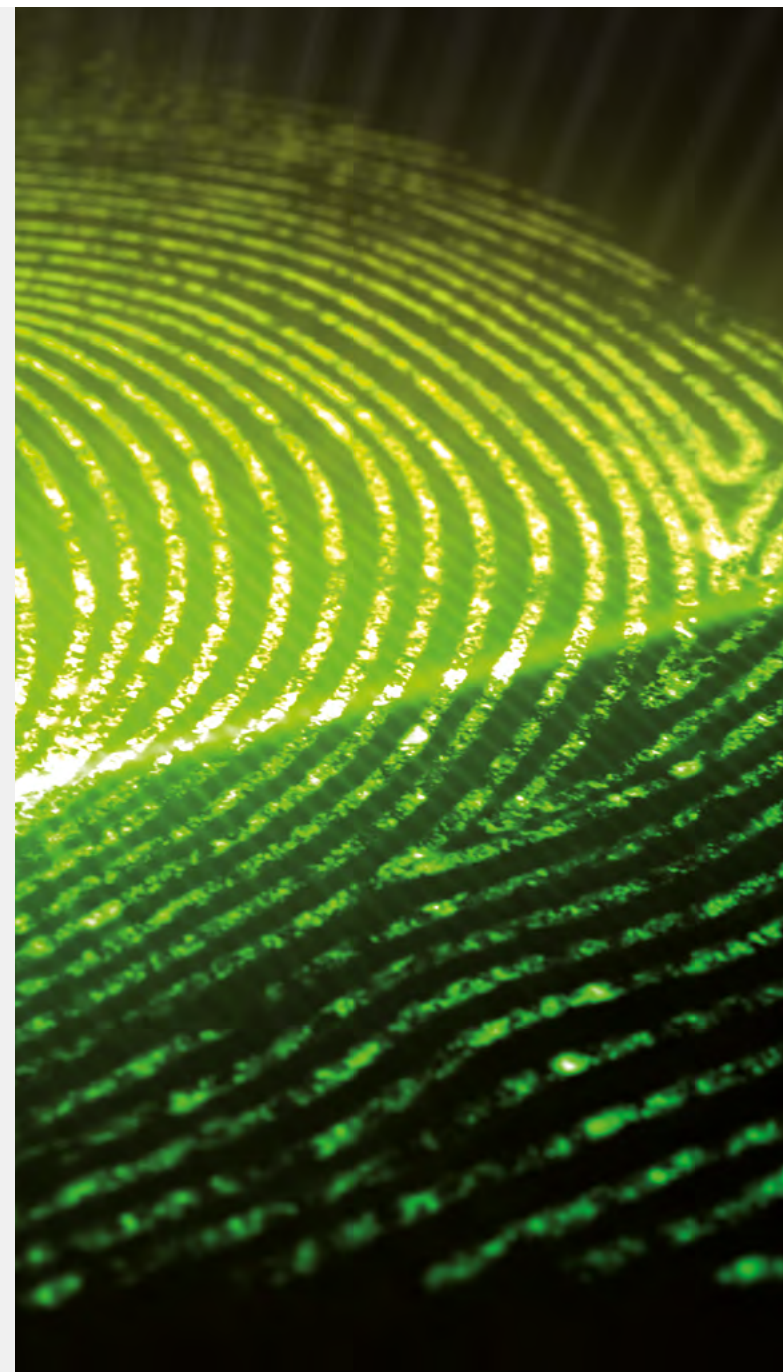


## E-identification / e-signature

E-signature is the electronic equivalent of a handwritten signature whereas e-identification is the process of using personal identification data in an electronic form which uniquely represent either a natural or legal person, or a natural person representing a legal person. In the EU many Member States provide their citizens with electronic IDs via smart cards, a citizen card to access public online services or others technologies such as mobile devices, or a combination of card and phone.

The Regulation (EU) N°910/2014<sup>11</sup> on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) was adopted in July 2014. Its purpose is to enable secure and seamless electronic interactions between businesses, citizens and public authorities and increase the effectiveness of public and private online services, eBusiness and electronic commerce in the EU. Many positive opportunities are provided by e-identification, for instance, in terms of security. Nonetheless, in practice, a number of legal obstacles remain.

11 [Regulation \(EU\) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market](#)



## Opportunities

- **Trusted e-identification and e-signature are paramount** for the development of the digital internal market and will offer numerous opportunities for the banking sector such as: facilitating access to distance product and services for consumers and the verification of customer identity.
- Mutually recognised electronic identification in the European Union can facilitate cross-border provision of many services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.
- E-identification and e-signature also contribute towards including citizens within a digital culture and creating an interoperable system involving all sectors.
- E-identification/e-signature also reduces paper volume and creates a more efficient operational system.
- **Banks have a widespread experience in establishing digital identities**, which places them in an ideal position to deliver digital identity services for business purposes and for the wider context such as partnerships with public authorities.



### What do e-identification and e-signature mean?

E-signature is the electronic equivalent of a handwritten signature whereas e-identification is the process of using personal identification data in an electronic form which uniquely represents either a natural or legal person, or a natural person representing a legal person..



### Positive role of banks in eID

In certain countries a major part of the success of eGovernment has been due to the implementation of eID by banks

## Barriers

- A number of banks already use e-signature as a way to complete the process of signing a contract (e.g. using a graphometric signature on tablet). In some Member States banks are currently using the e-signature as way to complete the process of Know Your Customer (KYC) identification imposed by the 3rd Anti-Money Laundering Directive in case of a non-face-to-face business relationship. Nonetheless, banks still need to collect copies of ID to complete the identification process. They are obliged to ensure a further check of the data acquired (enhanced customer due diligence), in a manner deemed appropriate to the specific risk.

We also observe that **inconsistencies exist within recently adopted EU legislations chiefly with regards** to the eIDAS Regulation 910/2014 and the 4th Anti-Money Laundering directive newly adopted. (See *EBF Blueprint chapter on removing regulatory inconsistencies*.)

New regulation on e-identity should include existing regulatory requirements and aim at enhancing and improving the identity process. Regulators should bear in mind that the digital development is moving at a very fast pace and adaptable regulation is key to providing a level playing field between banks and other less intensively regulated financial service providers. When it comes to issuing, verifying and exchanging data, equal enforcement and coordination between Data Protection Authorities and Financial Supervisory Authorities are essential.

- Identity theft is a strategic tool used by criminals. Thus, **all processes put in place for acquiring the e-identity should comply with a high-level of security and take into consideration the sophisticated nature of the crime**, especially, if public authorities generalise the use of an e-identification/e-signature. Undeniably, it appears more difficult to falsify traditional paper documents than electronic documents. Finally, securitisation of administrative documents should be guaranteed across all EU Member States.
- **Removing existing barriers to the cross-border use of electronic identification is key.** The e-signature is neither valid across markets nor from one country to another. If the digital solution is not trusted across markets it is difficult to find and establish customer friendly solutions. Favourable conditions should be created to ensure the interoperability of electronic identification such as work on standards, technologies and processes, and finding a convergence between the different sectors involved. In this regard, it is worth noting the European STORK 2.0 (Secure idenTity acrOss boRders linKed 2.0) project, aimed at realising a single European electronic identification and authentication area. The STORK 2.0 project is testing the opportunities of the cross-border use of eID in four key areas: eLearning, eBanking, Public Services for Business and eHealth.

- **The legal effect of an electronic signature should not be denied on the grounds that it has an electronic form**, as provided by the eIDAS Regulation. We observe that certain national authorities and regulators are reluctant to recognise officially private identification keys as a proper and legitimate form of client identification. The identification keys provided for clients by the banks should be a valid substitute for signatures used in business dealings with clients and not only for payment transactions in EU jurisdictions. Short of establishing a common e-identity and e-authentication system, digital signing of documents should be mutually recognised across borders as having the same legal status as physical signatures.
- **Safeguarding information over extended periods of time and guaranteeing the validity of the e-signature irrespective of technological changes are important elements to keep, notably for legal purposes.**
- **In addition, it is essential to create awareness and develop understanding through strong communication within a company and towards citizens at large.** A common framework for electronic archiving, with the same legal effect for e-signature and registered e-mails throughout the EU, could significantly reduce the cost and administrative burden of document retention.

## RECOMMENDATIONS

### E-identification and e-signature

- 1 Establish a truly interoperable environment with the recognition of a preferential use of cross-border national eIDs.**
- 2 Encourage trust in e-identification: further guarantees on the degree of trust in e-identification means ensuring that the person claiming a particular identity is in fact the person to whom the identity was assigned. Remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels to guarantee: a) the reliability of the environment in which the e-signature is created; b) that the e-signature is used under the sole control of the signatory.**
- 3 Establish common standards for document authentication and procedure to ease the use of e-signature at domestic and cross-border levels.**
- 4 Establish a common bank industry standard to allow the use of eIDAS under SEPA and the future PSD2.**



## Digital skills

### Competencies & talent recruitment

Digitalisation of the world of work is no longer a vision but a reality in full swing. It should also be the case for digital-ready personnel management.

Surveys among bank employees in Member States demonstrate the high awareness of the upcoming changes and a positive attitude towards these developments. A clear majority of employees rate that opportunities outweigh the risks. Employees constitute a solid basis on which to build this new and even more digitalised world of banking.





## Opportunities for employers and employees

- Digitalisation will guarantee that banks will continue to require highly skilled personnel and provide jobs that are both challenging and rewarding. This is not only evidenced by the need for a high level of IT-knowledge but also of general knowledge among customer service staff. **Flexibility and ability to learn and adapt to change will continue to characterise bank employees.** And, in more and more areas interdisciplinary knowledge will be a crucial factor (e.g. customer service, compliance, risk, etc.).
- The development of digital skills can be considered as central in paving the way to digital banking success. This means that the diffusion of an open digital culture inside the bank could help improve services and develop new business ideas.
- A key point is related to the area of talent management: business innovation is often the fruit of fresh thinking and new approaches. Banking organisation around digital services should encourage a process of wide-ranging ideas, involving different professional profiles and skills.
- A new scenario is arising: in the area of knowledge management utilisation of “swarm intelligence” offers new opportunities (i.e. most knowledge can be found within a community rather than in a book or a single person’s mind; and with the new technologies people in groups can work simultaneously on the same subject and be more efficient).
- Increased opportunities for even more flexible working conditions: working from home regardless of country and time, part-time job, etc. This includes enhanced opportunities to align working life with private life through increased flexibility.
- Technology continues to increase job opportunities for all skilled people, including those with special challenges (e.g. with disabilities).

## Barriers for employers and employees

- Work across borders, time zones and cultures will continue to increase. Likewise, the number of teams coming from various educational backgrounds. The convention of work performance being concurrent with physical presence will become less the norm. Banks as employers will have to continue to develop and update their personnel management, including relations with employee representatives at all levels, to match the changes and challenges that digitalisation will bring. One of these levels is the European Sectoral Social Dialogue for the Banking Sector<sup>12</sup>.
- As a result of digitisation, **future work in the banking sector will be increasingly mobile, spread out in multiple physical locations and carried out in virtual teams. This requires new working methods and skills.** Consequently, this generates learning needs for leadership and management, shifting focus away from traditional managerial duties and conservative leadership culture to coaching leadership combining training and leadership. Management skills will also have to adapt to the changing environment and diverse employee mentalities, especially those of digitally expert employees.
- **At management level more efficient decision-making structures are required** (i.e. rapid prototyping to foster creative ideas, fast decisions and parallel development of products and services). Boundary management (between working life and private life) will require digital ready policies and knowledge management will need to be developed so that knowledge is acquired by the organisation as a whole rather than by one person only. Indeed, knowledge management should become a core component of personnel management, as knowledge is often tacit, unstructured and difficult to formalise.
- What is more, diverse employee groups (with respect to skills, age, culture etc.) will provide further challenges. Digitalisation will offer job opportunities in banking for career changers, especially those with superior knowledge in statistics, mathematics, data-analysis, artificial intelligence/robotics etc.

<sup>12</sup> [European Sectoral Social Dialogue for the Banking Sector](#): the Social Partners have agreed on joint texts that deal – among others – with skills in the wake of digitalisation (IT-Employability, 2002) and with Lifelong Learning 2002 (to be followed up on 6. November 2015).

- In order to take advantage of new technological paradigms (Big Data, Cloud Computing, etc.), it is **important to understand which skills are required and where expertise can be found. Strong technological skills are not sufficient, it is also fundamental to develop other skill profiles**, such as business understanding, deep analytic skill, risk and cost awareness, and many others. In line with the Grand Coalition for Digital Jobs<sup>13</sup>, a study on digital skills in the workplace was launched in March 2015 by the European Commission. This initiative will allow social partners in just a few months to obtain a picture on the digital skill needs for the workforce. The study is expected to produce an estimate of the proportion of jobs in the EU that require digital skills. It will also include a set of job profiles exemplifying occupations for which recent developments in ICT and/or its use have caused a major change.
- The consequences of a more demanding work environment (speed of transactions, constant need to keep up with technology/product changes, increased availability of employees through various communication channels) have to be mitigated in so far as they have a negative impact on work performance and health.

## RECOMMENDATIONS

### Competencies & talent recruitment

- 1 Build a map of skill profiles to understand the strengths and weaknesses of a bank's knowledge environment and the main gaps to fill in.
- 2 Introduce the implementation of a structured change management process.
- 3 Improve job rotation practice, to help incentives for knowledge exchange and to build multi-skill professional profiles (e.g. through structured job rotation).
- 4 Improve employee's skills and competencies via training initiatives focusing on the conduct of a digital/online business in order to guide customers through online product and services.
- 5 Strengthen a collaborative work environment suitable for knowledge exchange and innovation.
- 6 Investigate social structures inside the bank (using for example social network analysis methodologies) to understand and map how knowledge flows through processes and organisational silos.
- 7 Adapt personnel management skills to provide a professional home-base for employees within a more flexible (place/time/content) work environment. Foster impact assessment of regulation on the employment relationship and have the employer's voice considered.
- 8 Promote IT skills and competencies via internationally recognised certifications, university careers, and internships within the banking industry.

13 [Grand Coalition for Digital Jobs](#).

## Digital Education

The Digitalisation process is key to enabling competent customers to manage money, keep track of finances, plan ahead, and stay up to date on financial matters. Interactive and easy to use online resources and tools help consumers to obtain information (i.e. financial products comparing tools), to budget (i.e. budget calculators), to borrow (i.e. debt tests, loan calculators), and to plan (i.e. financial “healthcheck” and pension calculators).

In 2015, the European Banking Federation (EBF) launched its first edition of the yearly European Money Week<sup>14</sup>, the aim being to raise awareness on the importance of financial education across Europe. Raising awareness on the importance of financial education in the digital environment will be part of future editions.

<sup>14</sup> [European Money Week](#): it is a joint initiative by European banking associations that aims to raise public awareness on financial literacy and improving financial education for students from elementary and secondary schools. The week consists of a series of events in the participating countries and at a European level.



## Opportunities for banks and customers

- **Banks actively support all customers including non-digital, analogue-minded clients who find it difficult to embrace new digital services and online banking.** For example, several banks teach elderly people about the “Internet environment” and help them to access and use online banking services, proposing special teams of employees available to support clients and help them with digital services and internet questions.
- Financial education programmes (available online) also constitute a useful tool developed by banks. They should be developed further to help new customers to adapt or to manage their finances. **More financially competent customers will be able to pick and choose easily between products, and customers, generally, will be able to access and understand new products** proposed through digital channels. This development will contribute to better financial inclusion.
- Some banks in certain countries have been active in designing and implementing financial education programmes both for children and adults, developing content, methodology and tools. Some educational programmes designed by banks target children more especially. For example, the school programmes launched are based on a digital and interactive approach in line with the ICT Pedagogy. They are aimed at promoting cooperation between private and public bodies to facilitate experience sharing and to optimise resources. Demo and educational games are available to heighten digital and financial culture. Digital competency should be developed in Europe and consumers encouraged to explore the digital world and the part banking plays in it.
- By increasing efforts in this area, banks will be able to contribute to customers’ ability to access and use digital products, ensuring they are used as intended, and the full benefits of digitalisation, realised. Digitalisation will increase trust among customers in digital banking services and improve reputation and attractiveness of the sector by highlighting trustworthiness. Banks could benefit from a wider cooperation as these issues have a broader social dimension and are relevant for many other stakeholders, both private and public. It is a win-win situation, for banks, customers and public authorities who aim at having more digitally integrated clients and at preventing social exclusion.

*“Helping customers understand their money and the organisation’s proposition will instil a level of control and confidence.”*

Benjamin Ensor  
DIRECTOR OF RESEARCH AT FORRESTER



## Barriers to the development of more digital programmes

- **The main risk here lies with customers being left behind** the banks' quest for more digitalisation. Dealing with customers lacking the necessary financial know-how can represent a risk as they are potentially less able to make solid, enlightened financial decisions and more likely to run into financial problems. Banks will need to accompany their customers in embracing new digital services.
- Another important risk is that of **fraud and cybercrime**, not least for a public lacking understanding of how to use authentication methods and digital services in general.

### RECOMMENDATIONS

#### Digital education

- 1 Launch, with the EU and international authorities, initiatives to promote digital financial expertise in society as a whole.
- 2 Improve digital skills and financial literacy among children, starting with school programmes.
- 3 Raise awareness on benefits of digital products and services and cybercrime risks.
- 4 Start partnerships with other interested parties in this area to initiate forward-looking discussion on the benefits of digital financial education.



## Removing regulatory inconsistencies

While it is recognised that financial services regulation has played an important role in the stabilisation of financial markets, development of the internal market, and implementation of consumer protection, it is also a fact that overlapping, conflicting and redundant regulation has been issued in several areas. What is more, the current regulatory framework has not yet properly or fully addressed the development made possible by digitalisation. As a result, a number of inconsistencies have been observed which are potential obstacles to the Digital Single Market becoming a reality.

Thus, the existing legislative framework should be fully assessed and updated where needed to ensure that it is still fit for the purpose of the new digital reality. The quality and coherence of financial services legislation will in this way be improved without reducing the obligations contained in the aforementioned principles.

The next few years will see a large volume of lower-level regulation (level 2) finalised in the financial sector. This work involves national and European financial supervisors and will introduce a large amount of new and more detailed regulation into the financial sector. Lower-level regulations encounter the risk to introduce new obstacles to developing genuine digital services and enhancing Digital Single Market in the financial sector. Any new requirements should be thoroughly thought through so as to meet the needs of the digital environment. A change in approach to the digital single market by authorities is clearly needed in order to embrace the new digital reality.

Some inconsistencies are listed below, and whilst not exhaustive, they should serve as an indication of the necessity for a more encompassing consistency check to be conducted in the near future.



## Anti-Money Laundering Directive (AMLD) vs. e-Identification Regulation (E-IDAS)

- In order to prevent money laundering, banks have an obligation to check the identity of their clients (Know Your Customer (KYC) obligations) as required by the Anti-Money Laundering Directive (AMLD). The obligations, as recently reviewed by the new AML Directive adopted this year (2015), still favour the physical presence of the customer for identification purposes. This could contradict the current objectives of the Digital Single Market to build a smooth access to online products and services for customers whenever and wherever they wish. For example, some banks proposing online products were obliged to request that a copy of the customer's ID card be given to a national Post Office before they could contact the client. Technologies allowing for Digital on-boarding should also be considered as equivalent and valid identification methods.
- We indeed observe inconsistencies within recently adopted EU legislation notably between the eIDAS Regulation 910/2014 and the 4th AMLD recently adopted. eIDAS regulation clearly presents e-identification and e-signature as a new opportunity to facilitate the establishment of non-face-to-face business relationships. The 4th AML Directive, which is currently being transposed into national law, holds that entering into relationships with customers not physically present in a bank branch is inherently considered high risk<sup>15</sup>. The result is that banks, when selling digital services to new customers, must observe a more thorough KYC procedure than otherwise mandated. This may mean that customers need to provide physical copies of ID or other documentation before being able to close a deal. Such an intermediary step naturally eliminates much of the inherent advantage of digitalisation, namely, accessibility and quick and easy communication. In essence, this is a conflict between the old standard of banking being something customers do at their bank branch and the new standard being something done online. There is also a conflict between a move towards faster processing and more easily accessible banking products on the one side and the effort to combat money laundering and terrorist financing on the other.

Furthermore, a reliable and consistent cross-border identification system would help digitalisation efforts and cross-border provision.

*"If we want the European digital sector to thrive we should focus more on promoting a cultural change than on regulatory intervention."*

Kaja Kallas,  
MEMBER OF THE EUROPEAN PARLIAMENT

<sup>15</sup> [See Annex III paragraph 2 of the 4th AML Directive 2015/849 EU](#) "the following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 16(3):[...]2. Product, service, transaction or delivery channel risk factors [...] (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;"

## Consumer protection & security vs. New Payment Services Directive (PSD 2)

- The first Payment Services Directive (PSD) adopted in 2009 provided the legal framework for the creation of an EU-wide single market for payments. The EU institutions have recently reviewed the Directive to help develop further an EU-wide internal market for electronic payments via the adoption of the Payment Services Directive 2 (PSD2). A balance has been sought between sometimes conflicting objectives such as innovation, user security, market integration, data protection, competition and consumer protection.
- The new Payment Services Directive (PSD2) stipulates that the “account servicing payment service providers” (namely banks) shall make possible for “payment initiation service providers” (third-party payment providers) to rely on the authentication procedures provided by banks to initiate a specific payment on behalf of the payer. It means that third-party payment providers will have access to client accounts and customer data information via the banks’ infrastructure. **The challenge is to ensure security and privacy for both banks and consumers** will be affected in this new scenario. Indeed, the structure behind the functioning of certain payment initiation services/third-party payment providers potentially calls into question the banks’ measures to keep online banking secure, and per se, puts at risk existing anti-money laundering and fraud prevention measures already in place. A clear liability framework, as well as appropriate technical standards, should be implemented to face fraud incidents and data protection. (See *EBF Blueprint chapters on Digital Payments and better access.*)

*“You can’t use 18<sup>th</sup> century law for a digital world.”*

Andrus Ansip  
VICE- PRESIDENT DIGITAL SINGLE MARKET,  
EUROPEAN COMMISSION

## Fight against cybercrimes vs. Network and Information Security Directive (NIS) / Draft General Data Protection Regulation (GDPR)

- The Network and Information Security Directive (NIS) currently under negotiation must build on currently existing business practices with regard to security incidents' reporting. Indeed, the banking sector has already efficient monitoring and reporting structures at national level (e.g. Computer Emergency Respond Teams (CERTs), national central banks' cybercrime centres). For this reason, it seems appropriate that for the implementation of the NIS Directive the above existing structures be taken into account when defining the reporting authority.
- The current negotiations regarding the NIS Directive envisage a "national derogation clause" which could allow a Member State to define, within the same sectoral "critical market operators", which entity is under the scope or not of the Directive. Should this provision be adopted, a level playing field should be ensured by EU-wide common derogation criteria in order to identify which entity is in or out of the scope of the Directive.
- The Internet Service Providers (ISPs) and the Information and Communications Technology (ICT) providers must be included in the scope of the Directive as critical infrastructures. Indeed, the banking industry depends heavily on these ISPs and ICT providers who know the banks' products and systems best, and who can react and report more efficiently.
- Finally, within the proposed NIS Directive and the General Data Protection Regulation (GDPR) negotiations, the banking sector might have to report to various competent authorities. For instance, if the "major incident" includes personal information, banks would have to report to the data protection national authority and to the NIS national competent authority. This double reporting is unnecessary and is onerous for banks.
- Regarding cybersecurity, banks' priority project for exchange of data on fraudsters and mules could be blocked due to insufficient legal grounds. As mentioned in the EBF Blueprint's chapter on cybersecurity, the current Data Protection Directive and the future General Data Protection Regulation are restricting the direct sharing of indicators of compromises (IOCs) with personal information between banks. Banks would advocate a more proactive and efficient way to process data to share incidents between banks. There are already organised financial industry fora which share IOCs. Nevertheless, the sharing could and should be improved by allowing these fora to exchange IOCs with personal information. What is more, banks wish to have a one-stop-shop mechanism when notification is required as, currently, banks have to notify several authorities at the same time. Aggregation of incidents, at a single point of contact, when they are occurring in several countries within the EU and outside, needs to be fast and efficient from the legal point of view.

*"We've seen improvements but when you add it all together the result has not revolutionised true change in the way people make everyday transactions."*

Richard Fraser  
MANAGING DIRECTOR AT GLOBAL FINANCIAL  
INSTITUTIONS AND FIS



## Fraud prevention and creditworthiness assessment vs. Draft General Data Protection Regulation (GDPR)

- The legislation in force, such as the Consumer Credit Directive<sup>16</sup> or the new Mortgage Credit Directive<sup>17</sup>, the Capital Requirements Directive<sup>18</sup> and the 4th Anti-Money Laundering Directive<sup>19</sup>, impose the use of data on banks when conducting a creditworthiness assessment for risk analysis and for identification purposes (Know Your Customer). In order to satisfy the regulatory requirements linked to fraud prevention, anti-money laundering and the conduct of an objective creditworthiness assessment of applicant borrowers for thorough and safe lending practices, banks collect several kinds of data from their customers. National legislation often provides in extensive detail the kind of data that needs to be collected. Profiling is therefore a crucial tool for banks to prevent fraud and money-laundering or to support the development of "tailor-made" products or services for customers. Profiling, then, should not be perceived as simply negative. Rather, it is a measure based on a balance of interests: preventing criminal actions and building consumers' trust in the digital economy as well as developing e-commerce.
- Currently, a number of provisions in the draft texts of the EU institutions on the General Data Protection Regulation (GDPR), under negotiation, limit profiling and data processing implying that a large part of the data collected by banks will be difficult if not impossible to use. The result is, these provisions may contradict current requirements such as the abovementioned legislation and the new Payment Services Directive (PSD2) adopted by the EU institutions in June 2015<sup>20</sup>.

For instance, the prevention of fraud and credit worthiness assessment are not covered by article 5 on 'Principles relating to personal data processing' or by article 6 on 'lawfulness of processing' of the draft General Data Protection Regulation (GDPR). At the same time the new Payment Services Directive (PSD2) recognises in its article 84.1 a) on 'data protection' the prevention of payment fraud and allows the "processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud". The question may also arise why this cannot be extended to the prevention of other types of fraud.

*"I believe that we must make much better use of the great opportunities offered by digital technologies, which know no borders. To do so, we will need to have the courage to break down national silos."*

Jean-Claude Juncker  
PRESIDENT OF THE EUROPEAN COMMISSION

16 [Directive 2008/48/EC on credit agreements for consumers](#)

17 [Directive 2014/17 EU on credit agreements for consumers relating to residential immovable property](#)

18 [Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions \(recast\)](#)

19 [Directive 2015/849 EU on Anti-Money Laundering Directive \(4th AMLD\)](#)

20 [Final compromise text on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC – 2 June 2015](#)

The current article 20 on profiling regarding automatic processing within the Council's General approach agreed in June 2015<sup>21</sup>, grants a right for the data subject "not to be subject to a decision based solely on automatic processing, including profiling, which produces legal effects concerning him or her or significantly affecting him or her". Such a right to manual processing may limit the scope of digitalisation for certain financial products and could prohibit or restrict risk assessment as part of lending practices.

These provisions may also be an obstacle to the development of data analytics (*see EBF Blueprint chapter on data value chain/big data*) whereas data analytics could improve customer experience, cybersecurity, fraud prevention and more generally the fight against over-indebtedness in the conduct of the creditworthiness assessment.

- In the context of building a Digital Single Market, it is also important that the forthcoming General Data Protection Regulation and any other data protection legislation do not hinder the transfer of personal data intra-bank. This should apply even when the branches between which the transfer takes place, are located in different Member States. The same goes for transfer of data between a front office in one Member State and a back office in another. This also means that processing, storing, etc. of data should be regulated in the same way regardless of the Member State in which the receiver and the sender of data are located respectively.

21 [General approach of the Council of the EU on the General Data Protection Regulation, 15 June 2015](#)

## Different national consumer protection and contractual laws across the 28 Member States

As expressly stressed in the Digital Single Market (DSM) Communication<sup>22</sup>, one of the reasons why consumers and companies do not engage more in cross-border e-commerce is because the national consumer protection and contract laws differ throughout the 28 Member States and companies need to act in accordance with the host countries' national consumer protection laws. This is also true for the retail financial services markets, still very fragmented. This is mainly owing to the different consumer/investor protection rules, despite the EU initiatives on consumer & mortgage credit or payment accounts. Despite banks' willingness to develop cross-border activities, they have had to invest huge amounts to ensure they comply with the national legislation on a daily basis (especially as national legislation is subject to regular review). In this instance, the resources invested for compliance purposes are not invested in the development of innovative solutions. This situation prevents consumers from benefitting from the most competitive and innovative online offers.

A number of recently passed directives such as Consumer Credit Directive (CCD)<sup>23</sup>, Mortgage Credit Directive (MCD)<sup>24</sup> and Payment Accounts Directive (PAD)<sup>25</sup> all have elements of consumer protection, without a particular focus on digital banking. It is therefore possible, that these new directives do not adequately provide for banks moving ever closer towards digital platforms and services. To determine whether there are actual barriers to digitalisation requires in-depth analysis. Differing national implementation of these directives must also be considered, as these differences can cause barriers to both digitalisation and cross-border provision of services.

For instance the CCD article 16 obliges creditors to provide adequate explanations to the consumer on the proposed credit agreements and any ancillary service. This means that there is a risk that certain Member States implement the provision in such a way as to hinder digital banking. For example, requiring the explanation to be given face-to-face, in writing or some other way that is incompatible with digital banking.

### RECOMMENDATIONS

#### Removing regulatory inconsistencies

- 1** Conduct a 'fitness check' of existing financial services legislation to adjust to the digital market reality and ensure consistency
- 2** In the context of the 'fitness check' proposed, create a platform for discussion with European Commission's DGs to ensure consistency and that the initial aims are reached.
- 3** Ensure the Digital Single Market balances competition and innovation with trust and security.
- 4** Safeguard the right balance between data protection requirements and profiling for fraud prevention and creditworthiness assessment.

<sup>22</sup> [Final compromise text on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC – 2 June 2015](#)

<sup>23</sup> [Directive 2008/48/EC on credit agreements for consumers](#)

<sup>24</sup> [Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property](#)





<sup>25</sup> [Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features](#)



## European Banking Federation (a.i.s.b.l.)

56 avenue des Arts,  
B-1000 Brussels  
P: +32(0)2 508 37 11  
F: +32(0)2 511 23 28  
E: [ebf@ebf-fbe.eu](mailto:ebf@ebf-fbe.eu)

[www.ebf-fbe.eu](http://www.ebf-fbe.eu)  
[www.ebfdigitalbanking.eu](http://www.ebfdigitalbanking.eu)  
[#ebfdigitalbanking](https://twitter.com/ebfdigitalbanking)

 @ebf\_fbe  
 @european-banking-federation-ebf  
 @European Banking Federation  
 @European Banking Federation

### Contact

[Noémie Papp](#) Policy Adviser  
Consumer Affairs & Coordinator Digital issues

[Sébastien de Brouwer](#) Executive Director  
Retail Financial services, Legal, Economic and Social Affairs

Design [inextremis.be](http://inextremis.be) m5181  
photos © fotolia.com

# Driving the Digital Transformation

The EBF blueprint for digital banking and policy change

[www.ebf-fbe.eu](http://www.ebf-fbe.eu)

[www.ebfdigitalbanking.eu](http://www.ebfdigitalbanking.eu)

[#ebfdigitalbanking](https://twitter.com/ebfdigitalbanking)

