Nederlandse Vereniging van Banken

NVB reactie consultatie FinTech

General remarks from the NVB

Expectations of bank clients are changing. Primarily as a consequence of digitalization. Whether in the form of disruption, revolution or evolution, the fact that major changes are taking place in the banking sector as a consequence of new technology cannot be denied. Established banks, new FinTech companies, supervisory authorities and other parties are all jostling for position in the new banking landscape. What remains unchanged is the essence of the financial services as offered, up until recently, almost exclusively by banks. In other words, while the banking sector may change, the essence of banking remains the same.

Banking continues to be about keeping clients' assets and accompanying data safe, keeping a payment system operational, mediating between savers and borrowers (the transformation function of banks), and absorbing the associated risks. Banks are increasingly facing a variety of technology driven developments, which are changing client expectations and offering opportunities to banks to improve services. These days many business sectors, and therefore also banks, are facing so-called disruptive technologies, which are technologies that can be so powerful that they change entire sectors. These disruptive technologies usually concern the digitalization of existing processes and their uses in new areas.

What is new is that there are now providers in the form of FinTech and BigTech which offer clients alternatives for each of these core tasks (or parts thereof) which are based on new technologies. For each of the core tasks referred to, clients expect a more digital service and their wishes are becoming increasingly measurable and audible for financial service providers. These changes form a new basis, for both new players and existing banks, to truly place the client at the center, to serve them better by providing better, more transparent, cheaper and more reliable products and services. The technological developments and the changes in consumer behavior therefore not only constitute a threat for banks, but also certainly offer opportunities for an improved, more relevant service to clients. Banks that know how to make the most of these opportunities will be able to play an essential role in the new banking landscape.

A high percentage of banks views the possibility of partnerships with Fintech with great interest and act accordingly, with the objective to obtain concrete benefits that enhance specific key business areas, products and/or services by leveraging:

a) Cost reduction solutions: focused on cost reduction via improvement to processes or replacement of platforms/ IT solutions with either new business models or technologies;
b) Customer onboarding solutions enabling banks to attract and on-board new customers, to improve customers' relationship or to increase the offer of new and innovative products/services
c) Risk management solutions;
d) Cybersecurity solutions (e.g. fraud detection and data protection);
e) RegTech solutions; have the potential to transform the way financial institutions manage the regulatory environment. RegTech can lead to considerable benefits for financial institutions and supervisors by allowing new technologies to be used to address regulatory and compliance requirements more transparently and efficiently and in real time;
f) Processing solutions; in the payments and securities space. Allowing the testing of new technologies such as distributed ledgers is of paramount importance.
g) Distributed ledgers solutions;

The EC has to find ways with sector stakeholders to embrace digitalization and remove obstacles of local, EU and inconsistent regulations.

Financial services legislation at both EU and national level should be innovation-friendly and make sure consumer protection is guaranteed, so that a level playing field between actors can be achieved and maintained.

A European level playing field is key: "same services, same rules, same supervision". This means policy makers should consider the importance of ensuring that a regulatory standard is applied and supervised across all participating markets. The reason that the cross-border provision of retail financial services is rather difficult is because there are still too many differences between Member States. These disparities create uncertainty and therefore lack of trust for the unknown provider. We note that the lack of a uniform set of rules across the EU (mainly as a result of local deviations to EU law and/or gold-plating) harms consumer trust to shop across the border for financial products. Without trust in a regulatory level-playing field for financial services with consumers, cross-border shopping will not increase

It is crucial that the national and international authorities closely coordinate their policies We support the idea that the authorities engage in (informal) conversations, an open dialogue, with current and new market parties in order for them to better understand the legal framework in which they may act. It is also important that the authorities share their views pursuant to the conversations with the public.

The collection and analysis of data play a central role for FinTech and stresses the need for consistent, technology-neutral application of existing data legislation (GDPR, PSD2, eIDAS, AMLD and NIS).The need for clear guidance/rules on data-ownership, access and transfer is stressed as well as the need for more legal certainty without adding more and potential conflicting laws.

With respect to cybersecurity, the fundamental value of trust must be present for any information sharing relationship to work. This can be facilitated and fostered by the EC. To ensure trust exists in FinTech providers they must be able to meet the same cyber security standards as banks and other financial service providers, to protect the cyber resilience of the sector as a whole.

Nederlandse Vereniging van Banken

1. Fostering access to financial services for consumers and businesses.

Question 1.1: What type of FinTech applications do you use, how often and why? In which area of financial services would you like to see more FinTech solutions and why?

It is important to provide customers with more choice and better conditions by facilitating digital Fintech solutions for retail financial services. We see that customers are increasingly interacting with banks in a digital, at times even a digital-only way. As such, being able to offer financial services in a digital way has become the new baseline. We experience that both banks and non-banks are developing new and innovative customer services that will increase competition and consumer choice. Most Dutch banks are also developing their FinTech solutions and collaborating with FinTechs on the market. Digitalization in retail banking will increase accessibility and convenience for clients.

FinTechs see the niche and specialize in it, which means they are able to bring a solution to the market quickly. For the longer term, relevant FinTech applications are data analytics, AI, DLT, machine learning and robotics.

Question 1.2: Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc.)?

Yes

If there is evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services, at what pace does this happen? And are these services better adapted to user needs? Please explain.

Yes, we believe that those services are, in general, better adapted to user needs. It is not the automation in itself that contributes to fore-mentioned personalization proactivity, but the underlying algorithms that are able to identify specific client characteristics. FinTech offering these services are launched and attracting customers. Incumbents are slowly launching such advisory services as well. They differ, however, as to what exactly is automated (risk profiling, asset allocation, asset selection, portfolio monitoring, rebalancing, …). The services are clearly digital, but the use of AI is still limited. Peaks is a good example that reaches out to more/new groups of costumers, but doesn't show evidence yet in its current phase of development.

Question 1.3: Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required? For instance, should a system of initial and ongoing review of the technological architecture, including transparency and reliability of the algorithms, be put in place?

No, at the moment we do not think this is needed.

Please elaborate on your answer to whether enhanced oversight of the use of artificial intelligence is required, and explain what could more effective alternatives to such a system be.

We believe that only in exceptional/extreme scenarios enhanced oversight is needed. We think transparency of markets is first line of defense against imperfect systems and markets and even for fraudulent AI systems. We see a (known and obvious) downside to implement enhanced oversight and regulation: it will most likely slow down developments in this area. We believe that the type of oversight that is in place for IT systems applied by banks today are sufficient to address the risks embedded in AI solutions.

A known risk is algorithmic bias. Models cannot look beyond the data they have been trained on, so whenever the training data is skewed or too narrow (and this is often the case), the model output will be biased too. One should be aware that a model, how intelligent the output may seem, is a mere representation of reality. A model can help users grasp certain elements of reality (a prediction, a categorization) but don't necessarily show the complete picture. That is why a human in the loop is essential: we are, unlike machines, able to take into account context and use general knowledge to put AI-drawn conclusions into perspective. I can imagine new roles emerging that evolve around checking model output from a human point of view.

Question 1.4: What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?

This is a question that cannot be answered beforehand and differs for each case. In contrast to 'traditional' linear regression analyses, unsupervised machine learning techniques (which are more and more often central to AI) don't involve specifying the relevant variables beforehand. The self-learning algorithm will determine autonomously which variables contribute to a certain output (prediction or categorization).

Any information requirements should be proportional, depended on the amount of money, risk profile. This should, and in many cases is already, defined by local regulation on investment advice, i.e. suitability test and KYC requirements.

Question 1.5: What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

A mix of different measure is already in place. Of course companies active in the EU will have to comply with to the GDPR from May 2018, but we believe it would be beneficial for both individuals and society if companies also formulate their own (ethical) guidelines when it comes to AI.

In addition, explainability of model output remains a challenge. Deep Learning, a subset of machine learning that attracts a lot of attention nowadays, is not only known to be effective in learning from big volumes of data but is also known for being a 'black box'. Reconstruction on how certain model output was achieved is still a subject that requires further research. Also see our answer on question 1.3.

Question 1.6: Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding?

Yes

Please elaborate on your reply to whether there are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding. Explain in what way, and what are the critical components of those regimes.

The number of crowdfunding platforms has rapidly increased to more than one hundred over four years time, covering about € 300 mln. According to the Crowdfunding Register of the Dutch Authority for Financial Markets (‘AFM’), 13 platforms hold an AFM permit, meaning that the vast majority holds an exemption. Unfortunately, many platforms communicate on a very minimal level about financial risks, where the risks are often significant. The consultation document seems to suggest that there are only two permit categories: a temporary or a permanent permit. In the (Dutch) practice, we see that the market needs a growth-model, where regulation is being adapted to the specific event in place (test phase, client scale up, offering particular services).

Question 1.7: How can the Commission support further development of FinTech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance.

The Commission could create a 'level playing field' for banks an alternative players when it comes to the "duty of care" and "know your customer". This level playing field would beneficial for Fintech startups as well, because partnerships between startups and incumbent banks can act faster.

Question 1.8: What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

Fund raisers
- Clear description of activity, risk and competition
- State of the development
- Ratio's expressing the health/status of the company/initiative

Platforms
- Success rates achieved by the platform regarding funded initiatives
- The business success of funded initiatives
- Failed project and how failed projects will be handled and are handled (case study)
- Transparency of fee structures

Self regulation:
Financial services legislation at both EU and national levels should be sufficiently innovation-friendly and safeguard a sufficient level of consumer protection, so that a level playing field between actors can be achieved and maintained. We expect that self-regulatory initiatives will prove to be insufficient to obtain an adequate level of transparency and consumer protection for the fund raising/crowd funding industry. Taking into account the ease at which fundraising platforms can attract loans and investments from consumers (online) on a cross border basis (even from outside the EU) on one side and the material losses retail consumers could incur on the other side, standardized consumer protection and transparency requirements should be warranted.

Question 1.9: Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services?

Internet of Things will also result in opportunities and challenges for financial services other than insurance services. A wide variety of (sensor)data will be generated by a wide variety of machines. For example energy companies are looking into remotely identifying machines which use more energy than necessary (e.g. old refrigerators and vacuum cleaners). As a service financials could work together with energy companies to identify such energy (and cost) saving opportunities and provide combined advice with respect to energy efficient replacements and financing of new energy saving machines.

Question 1.10: Are there already examples of price discrimination of users through the use of big data?

We are not aware of such practices.

Please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

Not applicable

Question 1.11: Can you please provide further examples of other technological

applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

EuropeOne: a European borderless bank
Peaks: investing in low amounts and automated; a mobile only investment App for millennials
Bunq: a startup bank focused on app based services

An example of other technical applications that offer new services, are tools to help parents make their (young) children acquainted with (digital) money in a world where cash payments in bills and coins are getting obsolete very quickly

2. Bringing down operational costs and increasing efficiency for the industry

Question 2.1: What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players? What measures (if any) should be taken at EU level to facilitate their development and implementation?

Banks are increasingly facing a variety of technology driven developments, which are changing client expectations and offering opportunities to banks to improve services. These days many business sectors, and therefore also banks, are facing so-called disruptive technologies, which are technologies that can be so powerful that they change entire sectors. These disruptive technologies usually concern the digitalization of existing processes and their uses in new areas. Partnering with FinTech companies can be a way for banks to quickly test innovative initiatives and thereby improving the time to market. Partnering with FinTechs is also required as banks cannot develop all new technologies in house.

From the banks' perspective the following disruptive technologies, among others, are relevant:

***Advanced analytics**:* The term advanced analytics refers to techniques used to predict outcomes and find new correlations on the basis of large datasets, or big data. Banks can use advanced analytics internally, for example for portfolio risk management and for marketing purposes, such as reputation management and monitoring product launches.

DLT: Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions, and is typically public for all participants, whose activities are encrypted. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum. DLT offers the financial sector many potential benefits, particularly in the form of cost savings, but also because fewer intermediate parties are involved in transactions and because of the greater transparency and safety with regards to data and transactions.***Mobile:*** The expectation is that the mobile channel is going to be one of the primary channels for Internet banking, online payments and mobile payments in stores. Internet banking is already taking place on a large scale using mobile telephones and tablets, and Commerce (online payments on a mobile carrier) is growing rapidly.

Artificial Intelligence (AI): Banks offer various applications ranging from digital (robo) advisers, to answering client questions on the website, to advanced *trading* algorithms and fully automated, algorithm-based credit approvals.

Internet of Things: The 'Internet of Things' (IoT) is a network of physical objects equipped with electronics, software, sensors and network connectivity with which these objects can exchange and collect data. The IoT for consumer applications is dominated by issues relating to privacy and security. It allows banks to help clients through, for example, the use of bank identification for the online identification at other organizations such as government bodies or web shops, or through the safe authorization of payments via the IoT.

Cloud computing: The use of cloud solutions at banks currently varies from so-called *private clouds* (cloud solutions whereby the servers are used exclusively by the bank in question) to full use of the IT infrastructure to a public cloud solution. The possibility of being able to use the required IT infrastructure much more quickly, as well as the scalability, flexibility, and cost savings, are the main sources of motivation for banks to switch to *cloud computing*.

Biometrics: Biometric applications at banks usually concern authentication or authorization by means of human characteristics such as fingerprints, iris scans, voice recognition or even face recognition. Biometrics can be used to make it easier for clients to interact with the bank, for example by simple authorization of the payment or faster authentication ('I am who I say I am').

Robotics: Robotics is not only used when automating and improving current systems and processes, but also to improve the client experience. In addition to simple activities such as greeting clients, robotics enables client wishes and needs to be registered, and the best responses or solutions to be offered more quickly

Question 2.2: What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?

- As an overarching barrier which requires serious improvement we identify the diverging manner in which individual EU Member States apply harmonized EU laws relevant to financial services, use of data and innovation. This is a key problem, as this effectively results in 27 separate markets for financial services. Examples are known of, successful Dutch FinTech companies leaving the Netherlands and move to larger markets such as Germany in order to grow to the next stage.
- Make sure that financial service providers can work within the EU in a regulatory level playing field that leaves room for innovation. We still see differences in Member States regulation on Anti Money Laundering, banking secrecy, e-signature, language requirements etc. Local regulations are often rule-based and prescriptive, preventing innovative solutions. Also, we see gold-plating making a uniform product proposition difficult. We suggest that the Commission will further harmonize relevant EU regulations via maximum harmonization and/or – principle based - regulations, thereby preventing gold-plating and leaving room to financial service providers to come up with innovative solutions.
- With respect to security, key issues need to be addressed at European level. These include risks resulting from open data. Clear principles are required with respect to the roles and responsibilities of each individual participant in a chain. FinTechs, when licensed, of course need to comply with applicable requirements on business solidity and security in an identical manner as other licensed financial institutions in the same license category. The innovative use of technology warrants additional attention with respect to the risks relating thereto and the mitigation thereof. The latter also applies to unlicensed FinTechs. Security is a key point of attention for fintechs. When partnering with FinTechs, a problem we experience is the lack of common minimal security standards. We are therefore required to perform detailed due diligence and analysis to assess the risks and security level of each individual FinTech. Standardisation/common security reqirements (if feasible) would reduce these efforts and facilitate collaborations between incumbents and FinTechs. We need to ensure that any issues occurring at the 'weakest link' do not result in systemic risks

- The EU can facilitate the development & implementation of use cases for new technology in different ways:
    - Adjusting the regulatory environment to digital reality by ensuring that future and current legislation & regulation is technology neutral rather than technology-specific. E.g. having regulations with regard to privacy or outsourcing is fine, but stating that all use of cloud technology must be treated as an outsourcing is not proportionate: when assessing the risk related to applying a technology for a specific business process, it is not the technology that determines the risk but the business process;

- Stimulating regulators to take an active role in assessing and developing use cases by being involved (e.g. by joining projects, if only as an observer);
- Ensuring that regulators are willing and able to take a more pro-active role when new technology is considered, e.g. by entering into discussions with subjects about how legislation is to be interpreted (something that for instance the Dutch DPA ('Autoriteit Persoonsgevens') is currently not willing to do);
- Further barriers the EC can help break down include promoting and facilitating collaboration between incumbents and licensed and unlicensed FinTechs. This could be done by lowering/updating the requirements on outsourcing to FinTechs and creating clarity on license requirements of FinTechs, in particular with respect to the applicability of intermediary/brokerage licenses (see our answer to question 2.10 and 2.11 for more detail). Facilitating data transfers and making more flexible rules on personal data better suited for the digital reality.
- Stimulate the development of purely European cloud providers;
- Harmonize the regulations re outsourcing of financial processes/underlying technology throughout the EU. Currently the requirements vary not only by country, but also by type of financial institution (EU regulations contain different requirements for different types of FI's);
- Standardization efforts, which are key for market take up, competition and interworking. When needed enforcement of the use of standards (like in the telco industry in the 1990s), with the aim to speed up and promote market development, without killing the upsides for initiatives that take risks;

Furthermore, the EU could play a role in:

- **Streamlining harmonised format and procedures for security (IT) incident reporting** to avoid overlap and redundancy in reporting to multiple competent authorities (NIS Directive, PSD2, Data protection regulation, Single Supervisory Mechanism SSM).
- **For resilience purpose and risk mitigation establishing a legal framework for data sharing** which allows the possibility to sensitive information related to fraud & cyber-attacks at national and cross-border level should be put in place.
- **Harmonisation of digital client onboarding**

Question 2.3: What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?

Automation and innovation do not necessarily mean a reduction on employment.
Digitalization will create demand for new skills and competences on general coding, machine and deep learning, data science, Blockchain, and (Cyber) security.
An important factor which needs to be addressed at EU levels as well as in each individual EU Member State, is education. In order to become a nexus of innovation, the European labor force needs to become far more digitally skilled. The end goal should be a substantial increase of the percentage of digitally skilled persons and IT specialists leaving European universities and colleges with a diploma and a robust digital skill set each year. Focus on digital skills should start at elementary school for each child in the EU and continue through the complete education program, irrespective of the level.

Financial institutions, but this applies to all employers in the EU are facing serious difficulties attracting a workforce with the right Digital/IT skill set. We expect that the global demand for highly skilled IT professionals will only grow in the coming decades. Apart from legislation, an important factor which needs to be addressed at the highest EU levels as well as in each individual EU Member State, is education. In order to become a nexus of innovation, the European labor force needs to become far more digitally skilled. The end goal should be a substantial increase of the

percentage of digitally skilled persons and IT specialists leaving European universities and colleges with a diploma and a robust digital skill set each year. Focus on digital skills should start at elementary school for each child in the EU and continue through the complete education program, irrespective of the level.

Question 2.4: What are the most promising use cases of technologies for compliance? purposes (RegTech)? What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?

RegTech has the potential to transform the way financial institutions manage the regulatory environment. RegTech can lead to considerable benefits for financial institutions and supervisors by allowing new technologies to be used to address regulatory and compliance requirements more transparently and efficiently and in real time. The most promising use cases we know are:

- -Combining regulation and cognitive solutions
- -Electronic identification and verification
- -Smart transaction monitoring
- -RoboAdvisor based risk assessment
- -The application of data analytics and so-called “big data.” These techniques can be used to reduce compliance risks in areas such as anti-money laundering. Big data techniques can identify potentially high risk customers (possibly in combination with biometrics to identify a client in a digital environment and/or authenticate a high risk transaction); make reporting information more accessible and easily searchable to regulators; improve internal culture and behavior by better identifying actions that could lead to compliance violations or incur reputational risks to the institution; and in combining big data with artificial intelligence, allow firms to reduce market risk through more precise modeling and forecasting of market trends and sentiments.
- DLT/Blockchain (e.g. Recording and storing information, Aggregating data, Performing operations on data, Sharing information with other entities, Ensuring data integrity)

Challenges are to build solutions that fit the regulators and the regulated financial service providers. It will be beneficial for auditors, incumbents and RegTech startups to collaborate closer to target the needs better. EU could promote standardization and promote standardized information. Financial institutions as well as the ESA’s and national competent authorities need to build up experience and expertise in these matters and use these technologies or otherwise ensure they are involved in initiatives relating to the development and implementation thereof, in order to adequately assess risks resulting from application of these technologies and the suitability of these technologies for compliance objectives.

Another challenge is unfamiliarity with the mechanics of the blockchain/DLT and/or a lack of clarity of the characteristics that will be attributed/programmed therein. Therefore uncertainty exists with respect to the manner in which compliance goals can be achieved using DLT, the escalations which occur when compliance cannot be achieved and the actions we should take to address such non-compliance/non-conformity. Ownership of the blockchain and responsibility for the block chain are also serious challenges. Who will be responsible in case of fraud and who will be liable? To which party should a consumer turn to get compensation/redress? The above questions also arise to some extent when using Big Data and AI solutions for compliance purposes. Financial institutions need to build up experience and expertise in these matters.

Question 2.5.1: What are the regulatory or supervisory obstacles preventing financial

services firms from using cloud computing services?

Also with reference to our answer to question 2.2

In The Netherlands, the use of cloud computing is constrained due to the Dutch Central Bank Circular that states that all cloud computing initiatives must be treated as an outsourcing. This policy is too broad, as it means that also for processes that wouldn't be considered to be an outsourcing in case other technology than cloud computing would be used, are now subject to outsourcing requirements. In our view, the outsourcing regulation itself adequately determines when delegation of a process is outsourcing or not, thus ensuring that adequate control measures are put in place in all scenarios.

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

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

The above issue may be mitigated by EU legislation resulting in harmonisation and minimum requirements applicable to such CSP's, and perhaps an EU passport/license, which takes into account the specific characteristics of cloud services. The latter would also be beneficial to CSP's as they could roll out their business with EU financial institutions pan-European, while having to deal with only one regulatory regime and one home regulator.

In general, cloud service providers are unwilling to accept instruction rights for financial institutions that may require the CSP to change the manner in which it provides its services, as they offer standard services to all their clients. Also, in general, CSP's are unwilling to agree to always enable financial institutions to meet the laws and regulations applicable to such institutions. Also, some large CSP's are unwilling to agree to direct audit rights for financial institutions and these institutions may only exercise such through review of SOC2 type 2/ISAE 3402 type 2 audit reports issued by the CSP's auditor.

Question 2.5.2: Does this warrant measures at EU level?

Yes

Please elaborate on your reply to whether the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services warrant measures at EU level.

The Commission should continue its positive work under its Free Flow of Data Initiative to remove unnecessary data localization requirements, except where necessary for legitimate public interest reasons. Not all banks experience issues with suppliers/providers to incorporate the EU model clauses in their contracts. However, some see that getting assurance statements/reports is still challenging and not standardized yet, it takes a lot of effort and time to get them and the level of quality differs per provider. Cloud computing is a technology, not a specific business process. As

stated in the three core principles, the EU should ensure that legislation is technology-neutral. This implies that any regulations for FI's specifically focused on cloud computing must be withdrawn (see answer on 2.5.1).

On the other hand, it could help if generic obligations were created that apply to cloud service providers that provide cloud services to FI's (.e.g. comparable to how the Global Data Protection Regulation now contains obligations not only for data controllers but also for data processors).

Question 2.6.1: Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with?

Yes

Please elaborate on your reply to whether commercially available cloud solutions do meet the minimum requirements that financial service providers need to comply with.

Key requirements (apart from best practices applicable to any business critical/important contracts) come from outsourcing requirements and privacy legislations. More and more, public cloud providers understand the specific demands from FI's re cloud computing and to a certain extent are able to cater for them. Public cloud providers sometimes meet the minimum requirements; some are more advanced in this than others but it is never easy to ensure all requirements are met. Note: the bigger the cloud provider, the harder it seems to be.

The market for some specific cloud services, like IaaS and PaaS, is highly concentrated, and risks being dominated by a few very large and powerful suppliers in the near future. Individual EU financial institutions (even the largest ones) have very little room to negotiate amendments to the standard contracts provided by these large Cloud Service Providers ("**CSP's**"). In general, large CSP's are not willing to make any changes to their standard contracts and terms, especially to accommodate the requirements as explained in our answer to question 2.5. Rules applicable to EU financial institutions should take this into account. Either the requirements applicable to EU financial institutions should reflect that there is little room for negotiation, or the EU should take action to demand that CSP's will take a more flexible approach, when contracting with EU financial institutions or regulate the large CSP's that expose European financial institutions to a substantial concentration risk to make sure these comply with the relevant requirements.

Complex supply chains such as a SaaS solution built on another provider's infrastructure/platform also make securing rights to have access / to interview personnel (for each party of the supply chain) challenging in negotiations. Effective identification, monitoring and reporting of risk is thus more challenging in many cloud environments given the lack of visibility over the whole supply chain of the technology stack.

This challenge is further driven by an ambiguity concerning how far auditing rights should be exercised throughout the supply chain. Without clarity concerning what is required to comply with regulatory requirements, banks may either look to secure rights extensively all the way down the supply chain, or may, on the other hand, be forced to take on additional risk in not securing extensive audit rights.

The challenge for cloud providers is compounded by the large number of customers and by the standardized offering which leads to a high level of complexity when giving individual customers the right to audit.
As a result, effective identification, monitoring and reporting of risk is more difficult in many cloud environments given the lack of visibility in the whole supply chain of the technology stack.
Besides the CSPs' operative responsibility around service provisioning, banks as data controllers are liable for the data stored and processed. As such, cloud service consumers need assurance that all contract terms are fulfilled. However, some CSPs are not always able to comply with specific contract terms, such as the right to audit. Hence, a common regulation agreement should be developed so as to facilitate compliance with a commonly understood set of minimum requirements to operate in Europe.

Question 2.6.2: Should commercially available cloud solutions include any specific contractual obligations to this end?

Yes; right to audit and right to examine.

Please elaborate on your reply to whether commercially available cloud solutions should include any specific contractual obligations to this end.

On request. It is not up to the cloud solution provider (who generally provides the contract) which contractual obligations are applicable to it. This must either be determined by the FI, or, see answer at 2.5.2, by EU regulations.

There is room for improvement since we see that some providers/supplier only incorporate clauses after an explicit request and not in their standard offer / supply contract.

Question 2.7: Which DLT applications are likely to offer practical and readily applicable opportunities to enhance access to finance for enterprises, notably SMEs?

DLT applications in several areas could positively impact enterprises' access to finance, including SMEs; International payments, Trade finance and Digital Identity.
A good example of a DLT application is the Digital Trade Chain (DTC). Seven major European banks are partnering on a new Blockchain-based trade finance platform, with a tentative plan to launch sometime in the second half of 2017. Those backing the platform's development are looking to establish a secure place to manage open account trade transactions for both domestic and international commerce. DTC utilizes a permissioned ledger, with authorized parties allowed to submit transactions on the platform.
The aim of the platform is to make domestic and cross-border commerce easier for European small and medium-size (SME) businesses by harnessing the power of digital distributed ledger technology.

The DLT can provide a single source of information where SMEs can share their financial data (obviously complying with existing regulation, starting from GDPR) in order to help the financial institutions to better assess their credit risk. This could make easier for SMEs access to some banking services and especially financing services.
It could materialize via "Smart Contracts" - contractual clauses to be fully self-executed, self-enforcing, or both, used in highly standardized operations. In trade-finance and in invoice prepayments there are interesting applications supporting companies and SMEs.

Question 2.8: What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardization and interoperability of DLT systems)?

Each use case has different requirements in terms of confidentiality, privacy and scalability. One challenge lies in how to balance these requirement respective to current technological capabilities, which are of course expected to improve as the technology matures. On a similar note, we can already observe a certain fragmentation in the market which may lead to interoperability difficulties between DLT systems. Should a large number of solutions be developed that independently address different needs, interoperability becomes an even greater concern. On a similar note, interoperability with legacy systems is another aspect that needs to be further explored and can provide difficulties. However, due to the potential of cost mutualization in implementing DLT solutions, legacy systems would be easier to replace altogether.

Question 2.9: What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

The main obstacle stems from the lack of an official regulatory framework to guarantee the enforceability of smart contract from a legally binding perspective. Even if such a framework were to be developed at an European level, local interpretation may pose further issues. Indeed, developing such a framework is especially difficult due to a number of reasons:

- Unclear where liability rests in case of malfunctions
- The possibility of having no central authority administering the network on which the smart contracts are executed
- Some transactions within the smart contract may affect external elements / third parties (e.g.: intellectual property rights)
- Applicable jurisdiction / fragmentation

Considering the fact that there is no such thing as 'the Blockchain', because of the different types of Blockchain possible, it can be stated in general terms that there are two problems in supervising. 1) In principle, Blockchain do not recognize jurisdictional boundaries and therefore the question arises whether the supervising authorities could intervene effectively when necessary? 2) In principle, transactions on Blockchain are immutable/irrevocable: This would become troublesome for consequence management. E.g. what if a judicial authority could determine a transaction to be 'void' how the old situation could be recovered when transactions are irrevocable. 3) Any other specific issues to be considered are: - Privacy issues on personal data processed and which cannot be deleted from the blocks and thus will be public for as long as the Blockchain is in operation. - Who is to be held liable for transactions conducted on the Blockchain? All participants on the distributed ledger? Only a part of these? And if that is clear, how are you able to identify a client?

Beyond pure financial regulation, broader legal issues, such as corporate law, contract law, insolvency law or competition law, may impact on the deployment of DLT.
In particular we believe that with further development of the technology, the following regulatory issues might need to be addressed by regulators:

- Legal framework regarding the legal nature of blockchains and distributed ledgers in general, including territoriality (jurisdiction issues and applicable law) and liability (responsibility when something goes wrong)
- Legal framework for the recognition of blockchains as immutable, tamper-proof sources of truth regarding the information stored on it. Related to this, legal framework for the use of blockchains as single sources of trusted identity as well. Harmonized regulation about data protection and definition of identity in the case of legal persons will be needed as a previous step.
- Regulation on how the right to erasure ("right to be forgotten") shall be interpreted, because the tamper-proof feature of the blockchain collides with this right recognised by European regulation on personal data protection.
- Legal framework about the legal validity of documents stored in the blockchain as a proof of possession or existence.
- Legal framework about the legal validity of financial instruments issued on the blockchain.
- Legal framework for smart contracts in general, settlement finality and in international commerce in particular, including real-world enforceability, territoriality and liability.
- Legal framework about the treatment of shared information in blockchains from the perspective of cross-border flow of data, and data protection in general. Clarification on whether encrypted data is considered personal data is needed. Portability of personal data from one processing place to another.
- Legal framework regarding the use of the blockchain as a valid ruling register for the IoT.
- Regulatory reporting information standards definition on the DLT. Guidance on which regulator has an access to what type of data stored on the ledger and in which situation.

- Clarifications on the who should run the permission based DLT in the financial sector and who should control the access rights to the network. (e.g. a supra-national organization on a non-profit basis)

Question 2.10: Is the current regulatory and supervisory framework governing outsourcing an obstacle to taking full advantage of any such opportunities?

Yes

Please elaborate on your reply to whether the current regulatory and supervisory framework governing outsourcing is an obstacle to taking full advantage of any such opportunities.

Yes. At a certain level current outsourcing regulations codify 'common sense' requirements for such contracts. That is fine, but the way it is currently done is that the regulations are fragmented over countries and types of FI's (see answer on 2.2.), creating ambiguity re regulations when multiple regulations apply.

In addition, international intra-group outsourcing within financial institutions creates an even more complex regulatory landscape, e.g. when several foreign entities outsource a function to a central organization of the same FI, who in turn outsources it to an external service provider. This may lead to different local requirements being applicable to a centralized service, leading to significant inefficiencies for the FI's, but in setting up the service and operationally.
In addition, not all commercially available cloud solutions have come to an agreement on the right to examine with the Regulatory Authority, Dutch Central Bank ('DNB').

Question 2.11: Are the existing outsourcing requirements in financial services legislation sufficient?

Please elaborate on your reply to whether the existing outsourcing requirements in financial services legislation are sufficient, precising who is responsible for the activity of external providers and how are they supervised. Please specify, in which areas further action is needed and what such action should be.

Current regulations/requirements are sufficient, in the sense that there is no need for more/additional requirements. As stated above harmonization of outsourcing & privacy regulations would help a lot. The 'first' entity (in a chain of outsourcing entities), usually a customer-facing entity, is responsible for its own chain of outsourced activities.
Another important aspect is that EU legislation has not completely harmonised the intermediary/broker function. As a consequence, IT service providers and FinTechs may easily qualify as (licensed) intermediary in the Netherlands, when performing their activities under an outsourcing agreement. This means they may require a license. In order to promote cooperation between (unlicensed) FinTechs and licensed banks/financial institutions, diverging national rules, should be reduced to a minimum. In addition, clear EU level guidance specifying the circumstances in which a IT service provider or FinTech has to be considered as an intermediary/broker (and should be in scope of national Member State license requirements) would be beneficial. If the threshold for applicability of license requirements is set too low (e.g. a FinTech only transfers a consumers contact details and some general information on the product the consumer intends to purchase), this will substantially frustrate innovation. This should not be left up to the individual Member States.

Question 2.12: Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?

Blockchain can provide a lot of use cases bringing efficiencies for financial service providers

(and potentially also for a number of other industries). Currently the use cases more tested are relevant to Capital markets, Trade Services, Digital Identity/KYC and cross-border payments. Although not new, a relevant example is the use of API's.
Robot Process Automation could also reduce operating costs

3. Making the single market more competitive by lowering barriers to entry

Question 3.1: Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?

Currently, differences in local requirements regarding AML/CDD, e-signature, consumer protection, tax legislation, data protection/privacy (e.g. banking secrecy) make a centralized product approach difficult as local involvement or presence, either by an existing branch office, subsidiary or by establishing a branch office, in fact is still required. This limits innovation within these products and services and hampers the establishment of an EU single market.

For individual retail customers and SME's we face these obstacles most pressingly in the area of:
(i) customer on-boarding and the corresponding KYC and CDD; and
(ii) requirements for handwritten signatures in the case of some product purchases.

Solutions for these obstacles can lie in e.g. European wide acceptance of videoconference identification/verification or acceptance of derived customer identification via new possibilities under PSD2 and digital signatures for authentication of transactions.

We would also like to point out that some important prudential requirements are more punitive with respect to the provision of digital services as opposed to non-digital services. In particular, we find it unjustified that the liquidity requirements in the LCR Delegated Act impose a more stringent outflow requirement on 'internet access only' customer (deposit) accounts, implying substantially higher costs for a bank that is offering this product. From a prudential perspective there is very limited evidence that higher outflow percentages can occur as this is based on a limited data set. Also applying such a rule does not look justified, as it seems to be based primarily on a regulatory assumption that customers' funds can be withdrawn quickly, whilst in our current electronic era facilitating customer access is a generic feature for all customers.

Finally we would advocate for an amendment to the CRR. "Article 4 Definitions (115) now reads: "intangible assets" has the same meaning as under the applicable accounting framework and includes goodwill, with the exception of software for the purpose of Article 36 b)".

The banking industry faces digital challenges in competition with emerging technological players that do not have to face the heavy regulatory burden imposed on the banking sector and are free of prudential regulation altogether. The current regulatory capital framework for credit institutions does not recognize the value of software for capital purposes. The fact that every euro that an EU bank invests in an IT development needs to be backed is perceived as a significant disincentive for investments in innovation and a major factor of unfair competition.

We believe the investments in software should carry the same economic and financial rationale, regardless of the industry. Whilst this may not be sufficient, it sets the basis for the solution to the issue in the banking field. Evidence clearly indicates that software has value even in the case of liquidation of a bank. Software has become a core asset for the banks business models around the world. However, there is evidence of different regulatory treatment of software in some jurisdictions, including US where capitalized computer software can be recorded as an "other asset" and subject to regular risk rating and not deducted, therefore removing any artificial hurdle to banks investing in digital, creating value for the economy as a whole and leading worldwide innovation in the area. Furthermore, the European Commission issued decisions on equivalence of the regulatory regimes of third countries to those applied in the EU. Capital regimes of third countries that do not require

capital deduction for software has not been considered as an element of relevant discrepancy or inconsistency for the European Commission, neither for the Basel Committee under its Regulatory Consistency Assessment Programme. It lets us believe that the non-deductibility of software therefore does not raise an issue.

PSD II also results in issues which have not yet been addressed adequately. For example due to article 66/67 PSD II, it is unclear whether banks can require PSP's to agree to technical terms/conditions for use of API's and access to client data. In addition, due to article 94 PSDII explicit consent is required for the use of client data in each instance, this frustrates innovation. We are aware of the pressure from the FinTech industry to undo this.

Question 3.2.1: What is the most efficient path for FinTech innovation and uptake in the EU?

FinTech innovation plays a pivotal role in the "customer journey". From a customer point of view the digitalization of financial services is without any doubt beneficial as it increases transparency and reduces costs. The EC must find a way to mitigate the backward-looking effect of laws and regulation. Digitalization should be embraced and obstacles of local or European regulation that hamper digitalization (e.g. the requirement of physical identification and signature) should be removed.

The fragmented regulatory landscape can be overcome by further harmonizing regulations (e.g. AML, data protection, tax, consumer protection) by implementing maximum harmonization and/or regulations. We suggest that the EC further harmonizes relevant EU regulations by e.g. (i) preventing local add-ons and/or gold-plating and (ii) leaving room for financial service providers to opt for innovative solutions.

In order to ensure that trust is safeguarded across the industry it is important to assess which consumer protection levels apply. If specified consumer protection is in order this should be implemented on the basis of a level playing field between banks and non-banks. The same rules should apply for the same businesses. We deem it important that consumer protection is designed in such a way that it does not hamper the customer experience, but can be made an integral part of it.

To ensure a stable market environment it is important for service providers and regulators to work closely together.

We believe innovation requires sufficient room for partnerships between incumbents and FinTechs. EC initiatives should be aimed at facilitating these collaborations. Furthermore, divergences between the applicable regulatory regimes in the different EU Member States need to be drastically reduced. The Financial Digital Single Market needs serious work.

With respect to the national regulatory authorities, we applaud the initiatives taken by the Dutch and UK authorities, to facilitate innovation. We do not have a clear view on the initiatives in other EU Member States. In order to accelerate these initiatives, the European Commission could play an important role by facilitating the exchange of best practices and know how between national competent regulatory authorities, and keeping track of all the different initiatives to identify blind spots and overlap. We do not believe that promoting innovation through a top down EU approach, e.g. a EU regulatory sandbox will be effective. Structuring such a solution will likely take too much time. Furthermore, a one size fits all approach (e.g. by aggregating the requirements of each of the individual national regulatory sandboxes to come to a general standard) may not suit the needs in individual Member States.

There is a lot of uncertainty as to whether certain FinTech initiatives can be considered to be compliant with financial services legislation which has an inhibitory effect. A proactive approach of regulators could bring more certainty and thereby stimulate the deployment of FinTech initiatives. A level playing field should be ensured. It might help to have regulators exchange best practices, or publish opinions similarly to the article 29 Working Party.

Another inhibitory factor is market size being limited to the market of a Member State. FinTech startups are more likely to thrive in big markets with a lot of potential customers. Therefore, enabling cross-border provision of FinTech services will stimulate innovation through FinTech.

Question 3.2.2: Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants?

Yes

If active involvement of regulators and/or supervisors is desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants, please explain at what level?

The reason that the cross-border provision of retail financial services is rather difficult is because there are still too many differences between Member States in many other areas. These disparities create uncertainty and therefore lack of trust for the unknown provider. We note that the lack of a uniform set of rules across the EU (mainly as a result of local deviations to EU law and/or gold-plating) harms consumer trust to shop across the border for financial products. Without trust in a regulatory level-playing field for financial services with consumers, cross-border shopping will not increase. Also and for example, if foreign entrants in a local market are discriminated, this places them at a disadvantage and may lead to less cross-border market entry, including online entry. In this context it is important that 'Goldplating' is avoided.

Furthermore, we note that at this stage it is difficult to fully assess the impact the recently implemented EU legislative measures (Mortgage Credit Directive, Consumer Credit Directive, Payment Account Directive, Payment Services Directive, Interchange Fee Regulation, Data Protection Regulation, Network and Information Security Directive, SEPA Regulation (IBAN) and Anti Money Laundering Directive) in the retail financial services market.

Finally, Banks and Fintech Start-ups/non-banking Fintech are seeking to test out new technologies, solutions and business models but are constrained by the existing regulatory framework which does not allow low-risk and low-scale experimentation to take place under less stringent rules. This issue limits competition and may stifle innovation in financial services. Consumers, in turn, are hindered from enjoying certain improved value propositions from their trusted banks.
Regulators could help by exploring how to gear up in order to support innovation across its activities, working with industry and wider stakeholders. The authorities must provide Fintech start-ups and banks which innovate with leaner and faster authorization processes. A first step on this journey is to consider the creation of an EU framework for experimentation as safe spaces where regulated and non-regulated actors can test innovations in a controlled environment. It will provide a safe place for firms notably to test whether their new products are complying with certain requirements and the legislative environment is adapted to the digital reality. Furthermore, supervisors can pilot the overall digital transformation by helping new entrants within the process and enabling speed of launch. The analysis of the impact should be eased significantly and allows supervisors to continuously assess the safety and robustness of the financial services ecosystem. This regulatory framework for experimentation will allow the regulators to assess new products at an earlier phase and potentially amend legislation rapidly when beneficial to consumers.

Question 3.3: What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide the details.

Like banks, Fintech start-up and non-banking Fintech should be able to develop services available across the EU without incurring costs and slowing down the processes of adaptation of the services to each individual country.

The current regulatory framework for banks sometimes proves to be too rigid to fit in specific business developments. A clear definition of activities that are considered cross-border provision of services would be very helpful. Developments in the area of the electronic provision of services are going faster than regulation. In particular we notice a grey area between (or overlap of) cross-border provision of services and provision of services by way of a local establishment (branch office). A multichannel (or hybrid) approach both by a physical presence and digitally/online in some cases provides the best solution for a customer friendly approach, but it can require both a cross-border notification and a branch office notification. However, such a hybrid approach sometimes raises supervisory authorities' eyebrows. If a product marketed cross border by Group company A, with support of a branch of Group entity B, some supervisory authorities fear confusion for the client and prefer an "either/or" option. This may not always be possible and may form an impediment for the development (or at least offering) of new products or services. Institutions would be helped by either a less stringent approach by supervisory authorities and/or a regulatory framework that leaves room for such hybrid models.

Question 3.4: Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market?

If the EU should introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

We do not believe it would be beneficial to introduce new categories of financial services licenses specifically for FinTechs. The regulatory landscape in its current form is already highly detailed/granular and difficult to navigate. Adding new licensing categories will further reduce comprehensibility.

We advocate for an equal level playing field for all market parties. We support the idea that the authorities engage in (informal) conversations, an open dialogue, with current and new market parties in order for them to better understand the legal framework in which they may act. It is also important that the authorities share their views pursuant to the conversations with the public. Finally, in our opinion, it is crucial that the national and international authorities closely coordinate their policies.

Question 3.5: Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market?

Yes

If you do consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market, please explain in which areas and how should the Commission intervene.

<u>FinTech Cooperation</u>
In the cooperation between new and established parties, the operational risks of outsourcing are a potential risk to the sector. Complex technology services are regularly outsourced to a third party. Customer data and processes can be involved. Licensed services are subject to supervision also when these are outsourced to BigTechs or FinTechs. Parties should be aware of this. Supervisors should make sure that there is no uneven level playing field between the various parties with respect to the DNB cloud circular.

Banks impose the same rules on FinTechs as to other suppliers which should mitigate operational

risks. However, FinTechs that have a B2C model require stricter supervision. The (system) risks of small starting FinTech players seem limited at this moment, but to maintain the trust of the public in FinTech / Financial sector, supervision on FinTech players is important. We have seen issues with respect to FinTech in, among others, the US (Lending Club) and Sweden (Trustbuddy).

Data privacy
The supervisor may pay more attention to the protection of customer data in the supervision of new market parties. The NVB is also curious know what the role BigTechs is in providing access to devices.

Contribution to the public community
Banks contribute to public goals in various areas. This includes anti-money laundering and terrorist financing, anti-fraud prevention, sanctioning legislation against bad regimes or individuals. Banks also provide non-governmental data for income tax. We are interested to know how new market parties deliver services, how costs are shared and to what extent a level playing field is guaranteed between existing and new parties.

Systemic risk
In the long run, the impact of FinTech and BigTech on the robustness and return of the financial sector as a whole is an important factor. Maintaining public trust in the financial sector should not be under pressure due to possible shortcomings of FinTechs and / or BigTechs which could be prevented by the same level of supervision..

Consumer awareness and data privacy deserve extra attention. Transparency towards customers is very important in this respect. Together with the Dutch authorities we do not feel that proportionality in the supervision of FinTech in the area of security and privacy is necessary. We do understand the principle of proportionality for the supervision of this new young and fast-growing sector, however we feel that this should not be a reason to lose sight of the level playing field. To the extent that there is a lighter regime for the FinTech sector, we believe that a clear and well-motivated framework with realistic boundaries needs to be developed.

Decisions that grant limited custom permits or temporary exemptions (for experiments) should be published in order to inform all market parties. This should also be the case for - within the limits of competition law - formal or informal decisions with respect to questions from market parties regarding innovation.

Regulatory framework
See last paragraph of answer 3.2.2. on regulatory framework.

Question 3.6: Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market?

Please elaborate on your reply to whether there are issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market, and explain to what extent regulations on data localization or restrictions on data movement constitute an obstacle to cross-border financial transactions.

We are not sure what is meant by ‘implementing free flow of data’? Due to the General Data Protection Regulation (GDPR) there are not so many obstacles anymore. The GDPR intends to strengthen and unify data protection for all individuals within the EU. It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens and residents back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. A free flow of data will be supported by the right to data portability, provided by Article 20 of the GDPR. A person shall be able to transfer his personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. In addition, the data must be provided by the controller in a structured and commonly used standardized electronic format.

According to the financial rules on outsourcing for many EU countries, financial institutions must notify the supervisor and obtain their approval to launch cloud projects. This notification and approval has to be done on a case by case basis. It implies an indirect constraint to the free flow of data and, thus, to a faster innovation and a more agile cloud adoption. There is a need to harmonize EU financial supervisors' criteria when approving cloud projects.

Question 3.7: Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities?

Please elaborate on your reply to whether the three principles of technological neutrality, proportionality and integrity are or not appropriate to guide the regulatory approach to the FinTech activities.

We consider that the three principles are appropriate, but probably not sufficient. Technological neutrality is clearly desirable and facilitates the self-selection of the best technologies by market forces, although it is not sufficient to guarantee a level playing field. Proportionality is needed as a risk-based approach that takes into account specific activity risks, and not whole company risks by default. Integrity and competition are in the benefit of all stakeholders, and should always be promoted.

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

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

From a supplier's perspective, the concern is that a loss of trust by consumers in one area of the industry, whether that be a Fintech startup or a large incumbent, hurts the sector as a whole. With equal rights must come equal responsibilities. Cybersecurity is a good example of this principle. A failure by any single market participants hurts the reputation and damages trusts in the industry as a whole. Policy makers should consider the importance of ensuring that an internationally recognized standard is applied and supervised across all market participants. Regulatory guidance so as to avoid the "reinvention of the wheel" should be provided to avoid ending up with many different standards and further fragmentation. In anutshell, the concept of "same services, same rules, same supervision".

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

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

1.

Allow for competition to unfold: a number of adjustments to existing legislation / regulatory frameworks and right-sizing of regulatory requirements need urgent attention for competition and a Digital Single Market for financial services to take off, and must be addressed in the short term.

Put Digital first: a thorough fitness check by the EU of the existing complex regulatory framework is necessary to ensure it is fit for purpose to support banking in the digital age. To be clear we see no need to create new regulation for the digital era but consider it important to make a thorough and comprehensive review of existing legislation to ensure the current framework is up to date, future-proof and does not impede innovation and competitiveness in the Digital Single Market for financial services. Furthermore, regulation must not unduly constrain banks or Fintech startups from providing an effective response to the challenges posed by digitalization. In this context, it should be underlined that technology is moving faster than regulation gets updated, if the regulation is principles based then the innovation can continue without waiting for the legislation to catch up. For example there has been issues in the UK with people moving to all their utilities being managed digitally, so they had no paper proof of address documents which banks want for account opening. However government approved guidance was that paper documents should be taken rather than digital copies – had the guidance been principles based the issues with access could have been avoided.

2. Promote innovation and avoid unintended disincentives: regulation can also be observed as a disincentive to experimentation. Undertaking regulated activities in various Member States usually requires explicit permission from the regulator and approval of the way in which the firm in question goes about its business. A risk-averse regulator may not be willing to grant permission to unfamiliar or unproven business models. Unregulated entities may, however, find it easier to undertake new business without having to comply directly with the regulator's tests. Similarly, digital services can easily cross borders, and varying risk appetite among regulators and overseers may hamper the cross-border provision of services and unintendedly lead to market distortion.

Question 3.8.1: How can the Commission or the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation?

We feel that the development of practices and initiatives should take place primarily on a national level, however the European Commission and the ESA's can play an important role (i) in enhancing the exchange of best practices and know how between the different competent national supervisory authorities and (ii) in promoting the issuing of consistent guidance with respect to innovation/FinTechs in the different Member States.

We expect there would be merit in pooling expertise on specific topics/technologies. We expect this would have more benefit if this would be addressed jointly at the level of the competent national supervisory authorities (e.g. virtual expert pools on AI, DLT etc.).

Question 3.8.2: Would there be merits in pooling expertise in the ESAs?

Yes

Please elaborate on your reply to whether there would be merits in pooling expertise in the European Supervisory Authorities.

Pooling of expertise would improve and accelerate growth of knowledge/skills and make the behavior of ESA's more consistent.

Question 3.9: Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and

cybersecurity authorities) and consumer organizations to share practices and discuss regulatory and supervisory concerns?

Yes

If you think the Commission should set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organizations to share practices and discuss regulatory and supervisory concerns, please specify how these programs should be organized.

An “Innovation Academy” set up by the European Commission, coordinated by the ESAs and supported by financial (and non-financial) associations, could help to train subject matter experts with common background, able to spread the Fintech’s culture of innovation and to promote the development of innovative solutions.

These programs could be organized as follow:

- **Organization**: Nomination process through local authorities; participating teams not too large to ensure exchange and discussion;
- **Physical meetings** due to better relationship management; different EU countries as meeting place
- **Topics**: current issues of national or EU parties invited; future challenges and how to handle them; insights from experts to
- **Selected topics**
- **Method:** use modern, interactive and solution orientated methods and techniques (design-thinking, prototyping)

Question 3.10.1: Are guidelines or regulation needed at the European level to harmonize regulatory sandbox approaches in the MS?

Please elaborate on your reply to whether guidelines or regulation are needed at the European level to harmonize regulatory sandbox approaches in the MS?

We expect this would have more benefit if this would be addressed jointly at the level of the competent national supervisory authorities.

It’s necessary that all regulatory sandboxes in the EU work together and align with each other.

We believe national approaches are not helpful in a multinational and global financial industry. The main risk of a national approach might be to create a fragmentation with different approaches among the EU Member States, with the final result that neither financial institutions nor consumers can benefit from these initiatives. The development of exchange of good practices and the establishment of European guidelines or high-level guiding principles at EU level to harmonize regulatory sandbox approaches in the Member States could contribute to a convergence in domestic innovation policies across the EU, thereby facilitating the emergence of a single market for financial services.

Question 3.10.2: Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border?

If you would see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border, who should run the sandbox and what should be its main objective?

See question 3.10.1

Question 3.11: What other measures could the Commission consider to support

innovative firms or their supervisors that are not mentioned above?

See above

Question 3.12.1: Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision?

Although some standards seem to be appreciated e.g. Sepa and PSD II, there are a lot of technical standards, which may rather cause confusion instead of clarity. However, designating a certain standard with a mandatory or other legal qualification will sooner hamper innovation than promote it. Perhaps a registry of standards will provide some clarity.

Please elaborate on your reply to whether the development of technical standards and interoperability for FinTech in the EU is sufficiently addressed as part of the European System of Financial Supervision.

Question 3.12.2: Is the current level of data standardization and interoperability an obstacle to taking full advantage of outsourcing opportunities?

Please elaborate on your reply to whether the current level of data standardization and interoperability is an obstacle to taking full advantage of outsourcing opportunities.

See 3.12.1

Question 3.13: In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition- friendly approach to develop these standards?

More effort is needed on amongst others: API's, XBRL

Question 3.14: Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses?

Yes

Please elaborate on your reply to whether the EU institutions should promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses, and explain what other specific measures should be taken at EU level.

Good to have promotion from the EU institutions with respect to an open source model. We also believe that is beneficiary to promote commercial developments of/on top of open source libraries.

Question 3.15: How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

We see limited impact from the startups with the aim to compete directly. We see winning combination in startup + incumbent companies, due to mutual benefits. The incumbents companies have the customer basis and reputable brands, whereas the startups have agility and creativity. Uncertain factor in these developments is the Big Techs.

4. Balancing greater data sharing and transparency with data security and protection needs

Question 4.1: How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

The free flow of data is an important factor for successful innovation in financial services and the creation of a Digital Single Market for financial services. However, in our view taking down diverging national practices and undoing diverging national interpretations of EU legislation is a far more important factor.

The question whether services users should be entitled to fair compensation when their data is processed is fundamental and warrants more attention and background/guidance for interpretation than provided in the scope of this consultation.

Question 4.2: To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

The previous generation standards focused mainly on standardizing the format of messages that are being exchanged among market participants. DLTs include derivation of a set of shared facts into the standard, thereby eliminating certain kinds of mistakes and therefore lowering the need and costs of reconciliation and (manual) correction procedures. This focus on guaranteeing that parties agree on a shared set of facts can prove a very reliable way for storing and sharing valuable information.

Question 4.3: Are digital identity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services?

Digital identities are currently being addressed by the Dutch National Blockchain Coalition.

Please elaborate on your reply to whether digital identity frameworks are sufficiently developed to be used with DLT or other technological solutions in financial services.

From a technical perspective, DLTs are completely different compared to most other financial service technologies. For a DLT to leverage existing digital identity frameworks, it requires an identity provider to attest the identity of parties in a very specific way. In general this would mean identity providers / frameworks need to adapt or extend their technical offering to be compatible with specific DLT solutions. For most other technological solutions in financial services it could be said that financial services can adapt to the implementation details of the identity framework.

Advice, directions and standardization for a framework would be beneficial for all stakeholders. The EU can lead this effort.

Question 4.4: What are the challenges for using DLT with regard to personal data protection and how could they be overcome?

Compatibility of functionality and data protection rules

(1) Regarding this question, it's useful to separate DLTs in two streams: those that implement an everybody-knows-all information sharing policy and those that implement some way of selective broadcasting. In the first case, data is globally visible for all participants of a particular DLT, so it's not protected and therefore this flavor can be seen as fundamentally incompatible with privacy legislation (eg GDPR) Encryption may solve this problem, but it's uncertain whether this will actually be possible for all use cases. DLTs that implement some way of selective broadcasting do not have this problem.

(2) Regardless of the DLT flavor, current DLT solutions offer full availability historical transactions. This may or may not have a technical reason. For example, Ethereum has not implemented deletion

of historical transactions yet, but no fundamental reason exists that would prevent such behavior to be implemented in the future. In Corda, this potentially poses a bigger challenge, since historical states may be required to prove validity of future transactions, while personal data protection rules might disallow a party to retain certain information that is part of such states, effectively rendering it useless for the purpose of transaction validation.

Data Storage

A big issue is the location of the data stores. A list of trusted entities can potentially solve this issue. a.o. organizations banks can act as trusted entities.
Customers should have freedom of choice to find a suitable trusted entity, based on quality and functionality.

Question 4.5: How can information systems and technology-based solutions improve the risk profiling of SMEs (including start-up and scale-up companies) and other users?

The benefit of more efficient information exchange should be considered for the entire duration of the relationship between SME and the party needing the information. Search costs are only a small part of this. Moreover risk profiling of SMEs is combining public and private data sources. Access to cloud bases SME administration systems is essential and it is up to the SME to grant such access.

Question 4.6: How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers ? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?

Enriching data is a business model in itself and enhances transparency of the financial state of the SME. The risks from this potentially vast distribution of company data to a myriad of parties needs strict governance to protect SMEs. A bottom-up approach on the basis of the companies' financial data should be the starting point.

Question 4.7: **What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?**

The key point of departure ought to be the development of an equal level playing field. This means that 'new players' ought to meet the same requirements as existing financial service providers and market infrastructures. We have noticed a lack of oversight on FinTechs to determine their level of security and to identify insecure providers. The level of security, from our perspective, is extremely diverse which means there is a lot of work to be done to bring all of these players to an acceptable level. Therefore a level playing field is key, also in monitoring and supervision.

Question 4.8: What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

Information sharing from public authorities is limited. Reciprocity is a necessary element of information sharing, where both the public and the private sector exchange information whenever possible. Whilst we understand that during specific investigations, particular elements of cases cannot be shared, there also appear to be situations where there might be other factors at play to prevent information sharing.

Trust is a fundamental aspect to facilitate and enhance information sharing. The team to share with must be known, otherwise no trust will be given to team members. Trust can exist between individuals or intrinsically between groups who have similar purpose or experiences. Predictability about what is being done with the information is key.

Just sharing information would lead to more noise in the system, and would even help the bad guys, the haystack just grows and the needle gets harder and harder to find.
Identifying a shared interest or a common purpose is another crucial element. All parties participating in the information sharing must have a shared interest in doing so. Only when a common purpose can be defined (such as stopping a specific threat actor for instance) success can be guaranteed.

Another challenge is the volume of information shared and the different ways in which it is shared. The ability to share and subsequently digest the information in an effective way is therefore a work in progress. Fragmentation is still a worrisome factor in information sharing. Information can only be effectively shared electronically between systems. And most parties do not have Cyber Threat Intel systems based on standards like TAXII yet.

Question 4.9: What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

From a maturity perspective, the point of departure should be the assumption that criminals are able to enter the systems of the organization. The focus therefore ought to be on assessing how a business might be damaged when the unwanted visitors execute unwanted code. This is key and demonstrates the necessity to go beyond prevention and also invest in monitoring, detection as well as response and recovery. This implies testing is very context specific. It also implies that the focus upfront should be on learning and improving the threat analysis skills of the companies being tested. Improving the baseline is more important than setting a fictional baseline. EU coordination is only relevant to sustain a level playing field. These exercises are valuable but also require investment of resources such as money and time. Another element to consider is to test the entire chain of a transaction, to determine the resilience of the different parties involved.

Very important aspect to consider here is the significant shortage of competent professionals to do the test and the analysis. A roadmap should definitely ensure the needed investment on education is carried out prior to introducing more testing. The EU can play a role in helping to increase the number of professionals in this field.

Question 4.10.1: What other applications of new technologies to financial services, beyond those above mentioned, can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

Most issues are sufficiently covered in this consultation

Question 4.10.2: Are there any regulatory requirements impeding other applications of new technologies to financial services to improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

Please elaborate on your reply to whether there are any regulatory requirements impeding other applications of new technologies to financial services to improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?