Response of the Netherlands – Consultation document - FinTech: A More Competitive and Innovative European Financial Sector

This is a joint reaction of the Netherlands Authority for Consumers and Markets, the Netherlands Authority for the Financial Markets, De Nederlandsche Bank and the Netherlands Ministry of Finance, each institution with their own role and responsibilities.

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?

For Dutch examples of FinTech-technology, we would like to refer to overviews of Dutch FinTech-companies, such as provided by Holland FinTech.[1]

[1] https://hollandfintech.com/network/

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.) and at what pace? Are these services better adapted to user needs? Please explain.

Currently, no real quantitative evidence is yet available to support the stated claim that automated financial advice reaches more consumers, firms and investors. According to the laws of supply and demand, however, a drop in prices may lead to a surge in demand. In addition, innovation in automated advice can lead to greater accessibility. From this perspective, we already see market participants making preparations to offer products in the range of digital services and/or advice. Examples can be found in automated creditworthiness assessments for corporate lending, comparison websites that use personal data for targeted promotion and digital advice on mortgages, insurance and investment strategies. More specifically, the first automated mortgage advice is almost ready to go live and several (semi-)automated wealth management products are active on the Dutch market.

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? What could be effective alternatives to such a system?

In line with the requirements of MiFID-II for the possibility of auditing of algorithms in marketplace trading and the enhanced rights of consumers in automated decision making under the General Data Protection Regulation (GDPR), oversight over the use of artificial intelligence in decision making needs to be looked at closely. The use of Artificial Intelligence (AI) for decisions that directly affect consumers' lives is increasing, such as in creditworthiness assessments and investment portfolio's, as well as in financial planning. Also, AI may be used in processes that are central to the functioning of a financial institution, which may lead to possible risks for financial stability.

As many providers of these services operate outside of the traditional financial sector, the rules and regulations on the responsibility of subcontracting certain parts of financial service provision need to be looked at closely from the perspective of responsibility for the final advice. Also, cooperation agreements between the different National Competent Authorities (NCAs, being privacy, competition, consumer rights and financial services) need to be reached to come to fair supervision with the aim to further support the interests of clients of financial institutions. Developments, such as deep learning algorithms, challenge the current take on supervising algorithms. The European Commission may support developments in the area of AI, by initiating a discussion with Member States, NCAs and market participants on oversight over AI in the coming decade.

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)?

The acquisition of data should be in accordance with European laws regarding privacy (i.e. regarding redlining, and getting customer approval to use their data). Following the principle of technologically neutral legislation, requirements that apply to traditional advice should also be applicable to a digital process. This means that the principles of competence requirements that apply to physical advisors should also be applicable to automated processes. So, the set of data that a physical advisor needs to use to base an advice on should also form the basis for the minimum set of data that an algorithm uses for an automated advice. In addition, the provider should establish that the customer has significant knowledge about a product or service to enter into a contract, as is the case with physical advice.

Regarding the determination of e.g. risk, there have been examples for e.g. credit risk in the market ranging from very simple algorithms (based on 5 variables) to overly complex ones (>70 variables). In these cases, the solidity of the models /algorithms used (ability for back-testing, validation, supervisory control) is more important than the exact variables that are or are not included.

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?

Artificial intelligence and big data analytics pose new challenges on consumer protection and possible risks, as many of the possible uses of these techniques have yet to emerge. We would like to address three separate issues, namely robo-advice, algorithm-based lending, and the use of big data analytics in general.

1. On robo-advice, the Joint Committee of the three European Supervisory Authorities (ESAs) – EBA, EIOPA and ESMA – have published a report on automation in financial advice.[2] In this report the Joint Committee gives an overview of the consumer protection challenges and risks. The ESAs have concluded that they will continue to monitor this phenomenon given its growth potential, but have decided not to take any cross-sectoral regulatory or supervisory actions at this stage. In addition, the ESA's also note that financial advice in general is already addressed in various ways through a number of EU Directives. A forward-looking assessment of the need to further regulate automated advice is currently being performed by the Dutch Ministry of Finance together with the Authority for the Financial Markets, with results expected in the last quarter of 2017.
2. On algorithm-based lending, this activity may create the risk of inaccurate decisions and unfair treatment of particular borrowers, without giving them the opportunity to check and correct the data used in underwriting decisions. As is stated in the GDPR, a provider of these services should always be able to explain on which bases an automated decision is made, as is also applicable in the case of algorithm-based lending.
3. On the use of big data analytics in general, the Dutch government is preparing a response to the initiative report submitted by the member of the Dutch parliament Nijboer.[3] The reaction is expected to be sent to parliament in the third quarter of this year. The initiative report and the cabinet reaction may provide useful insights for the European Commission.

[2] https://www.eba.europa.eu/documents/10180/1299866/JC+2015+080+Discussion+Paper+on+automation+in+financial+advice.pdf
[3] https://www.tweedekamer.nl/kamerstukken/detail?id=2016Z22297&did=2016D45701

1.6. Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding? In what way? What are the critical components of those regimes?

We would like to differentiate in our answer between the three main forms of crowdfunding that are within the scope of financial regulation, namely 1) securities-based crowdfunding (sbc); 2) private-placement-based crowdfunding (ppbc); and 3) peer-to-peer lending (p2p), or crowdfunding in consumer finance.

1) MiFID already regulates securities-based crowdfunding at the European level, as was confirmed with the ESMA opinion of 18 december 2015.
2) Member states are currently implementing differing national regulatory regimes to introduce consumer/investor protection measures and prudential requirements for platforms that aim at the provision of private placement-based loans. The introduction of additional requirements is fitting with the development of crowdfunding as an alternative source of financing for businesses. As crowdfunding is still a mainly local phenomenon, European regulation of platforms is currently not in order. Guidelines and/or legislative actions for cross-border operating platforms in ppbc may be introduced in the middle to long term.
3) Regarding consumer credit provision through crowdfunding, we welcome the initiative within the framework of the action plan on consumer financial service s to examine the current regulation in the Consumer Credit Directive of innovative forms of consumer finance, such as p2p-lending.

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?

We welcome the current work of the European Commission on this subject, monitoring and analyzing current developments and meeting with stakeholders on a regular basis in order to accommodate FinTech solutions in the field of non-bank financing. Looking at the current market dynamics, it is key that the application of European regulation is predictable and consistent across borders. Supervisory convergence, supported by the ESA's, is important in this respect, as is technology-neutral legislation.

The European Supervisory Authorities may provide additional guidance in accordance with the National Competent Authorities on the implementation of different forms of alternative financing. As ESMA has provided her opinion on securities-based crowdfunding, the ESA's may provide clear and readable guidance for both NCA's and market participants to address possible unintended regulatory bottlenecks for innovation, while keeping consumer protection and financial stability at heart.

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?

We support the current levels of transparency in place in the Netherlands in which the AFM imposes additional requirements on platforms regarding transparency in general terms, on available information (should be clear and non-misleading) and on policies regarding risk-classification of loans, which can be found in the list below. Furthermore, platforms are required to continuously raise awareness of the risks attached to crowdfunding investments. Self-regulatory initiatives, e.g. of the industry association, are in place on top of these additional requirements and regulate e.g. information on default rates.

Below please find a list of elements that should, in our view, be covered at least when providing information:

- Description of the project / entity; it's activities, reasons of raising capital
- Risks relation to the fund raising entity
- Risks relation to the loan-parts / shares
- Information on guarantee(s) or pledges (if applicable)
- Default rates differentiated for expired / non-expired loans
- Description of the use of proceeds
- Information about natural persons behind the project (names, capacity, track-record)
- Financial forecast of the project / proposed yield
- (conflicts of) interest of natural and legal persons relating to the project
- Finance structure of the project / entity (other loans, equity, ratio equity-non-equity)
- (management and other) fees
- Way of administration of the loans / shares
- Rights and obligations attached to the loan-parts / shares
- Transferability of the loan parts / shares
- Risks relating to (the operation of) the platform

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?

In the Netherlands, the first examples of experiments with sensor data analytics and other technologies are emerging, e.g. in car and home insurance. The use of these types of technology in other types of insurance, such as health insurance (as seen in South Africa), have yet to emerge.

New business models based on these technologies lead to questions on fairness, solidarity and risk selection, which are also connected to the privacy of the individual. Furthermore, the use of new technologies may lead to new entrants in insurance markets, changing business models and possibly impacting the financial position of incumbent insurers.

As indicated out in our answer to question 1.5, the Dutch government is preparing a response to the initiative report submitted by the member of the Dutch parliament Henk Nijboer.[4] The response is expected to be sent to parliament in the third quarter of this year. The initiative report and the cabinet response may provide useful insights for the European Commission.

[4] https://www.tweedekamer.nl/kamerstukken/detail?id=2016Z22297&did=2016D45701

1.10 Are there already examples of price discrimination of users through the use of big data? Can you please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

-

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?

-

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?

We see the most promising use cases of FinTech in those (financial) processes that are defined by law, cover an information base from which periodic reporting is done, and include government as well as private sector parties. A successful implementation of such a process was done by the Ministry of Finance in automating the issuance of treasury loans through a smart contract, storing relevant data in a blockchain.

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?

Access to and standardization of information form a vital part to come to a fully interoperable infrastructure that supports both incumbents and new entrants to enable market participants to easily exchange data within the confines of the current (privacy) legislation. Supervisory convergence may be needed to clarify the interpretation of requirements in current legislation, such as requirements for client onboarding (Know-Your-Customer, Anti-Money Laundering and Anti-Terrorism Finance) through eAuthorization and eRecognition. The eIDAS-regulation is an important first step in this respect.

Secondly, FinTech benefits from economies of scale as is the case with most IT-services. The European Commission should critically assess looming concentrations of significant market power, such as in cloud computing, as this may have consequences for the stability of the financial system.

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?

-

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?

Although the compliance function is and will remain an integral part of a financial organisation's operations, the use of technology (including solutions from third party providers) can support and improve this function significantly. **T**he most promising use cases of RegTech concern: (i) automated reporting by banks and other financial institutions (eg the technical platform for the Austrian Reporting Services (AuRep)); (ii) the use of AI/machine learning to help financial institutions to understand their compliance obligations (eg. Using Watson to understand legal texts), as well as detecting potential inconsistencies between new and existing regulations at an early stage; (iii) the use of cloud based solutions (SaaS) that automatically update to the latest regulations in order to determine a financial institution's compliance obligations; and (iv) the use of DLT for internal control systems, which could also be used for auditing and compliance purposes.

Regarding RegTech the interests of industry, RegTech service providers and supervisors are to a large extent aligned (cost-efficient, automatization of compliance tasks, standardized information, improved data-quality, more effective use of available data, easy incorporation of new regulations, compliance by design), and successful use cases are readily available (eg. AuRep). For this reason, the EU does not need to actively support the development of Regtech.

However, the EU could facilitate the development of RegTech by initiating (or facilitating) a platform where industry, supervisors and the EC monitor and review potential barriers and opportunities regarding RegTech (e.g. the dissemination of data by supervisors and the format in which the European legal framework is made available), in order to create a RegTech friendly ecosystem.

Finally, an increased reliance on RegTech also harbours potential risks, and may pose challenges to future supervisory practice, such as:

- Concentration of sensitive information flows (of many financial institutions) could make RegTech service providers susceptible to cyber-threats.
- Concentration of compliance supporting functions within a small number of RegTech service providers could multiply the impact of potential failures by the RegTech service provider.
- The continuous evolution and application of AI in RegTech could raise questions about responsibility)regarding the compliance function of financial institutions).
- The day-to-day supervision of RegTech solutions (and the data provided by them) when they are offered by foreign (non-European) service providers as a cloud service.

2.5. What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services? Does this warrant measures at EU level?

In the Netherlands, Cloud computing is regarded as a specific form of outsourcing. Failure to comply with legal requirements or uncertainty about compliance may prevent financial services firms from using Cloud computing services. Other requirements, such as the need to notify supervisor DNB about the adoption of Cloud computing services, may cause delays in the adaption of Cloud computing services.

A specific example of non-compliance is adherence to the requirement on financial institutions to perform a risk assessment using a risk analysis framework and contractually agree to a 'right to examine'. In practice, risks are not always demonstrably presented and mitigated by a financial institution on a sufficient level, or not all IT outsourcing contracts stipulate an audit right for the supervisory bodies.

At the moment there are not many industry standards in place. These standards should be defined by the industry itself and may be facilitated at EU level.

2.6. Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with? Should commercially available cloud solutions include any specific contractual obligations to this end?

Currently this depends on the Cloud service provider's maturity level. In general, the majority of the major Cloud service providers meet the legal requirements and also want to comply with them. In practice smaller Cloud providers are struggling to meet the minimum requirements. It is of great importance that the supervised financial institutions evaluate and accept (residual) risks themselves.

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

-

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

As the first applications of Distributed Ledger Technology (DLT) are being introduced in pilots and small-scale projects, many of challenges are currently being identified. We currently see the following challenges for the wider implementation of DLT-solutions, as is also mentioned in our response to question 2.9:

- Overall acceptance of the technology (by a sufficient amount of market parties, sufficient efficiency gains and cost reduction potential);
- Technological challenges such as a sufficient maturity level of DLT, scalability, privacy, identity, interoperability (connectivity) with existing systems and processes, standardization, data management and protection (technological factors), security;
- Governance of the DLT system / network and adequate (new) agreements regarding maintenance (including updates) and obligations, liabilities and rights of the participants;
- Confidence in the cyber resilience of DLT.

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?

As stated in our reaction to question 2.8, the first applications of Distributed Ledger Technology (DLT) are currently being introduced in pilots and small-scale projects, so many of various regulatory or supervisory obstacles may still arise to the wider deployment of DLT solutions. We identified the following cases of usage in pre- and post-trade environments.

Issues may arise when a 'non-proprietary' DLT application (comparable to the one used in Bitcoin) is introduced in a securities environment regarding the legal ownership of the DLT and who can be held responsible for the system and the data in the system, as supervisory legislation targets institutions as owners of systems or providers of services, but a 'Bitcoin 'type of DLT is without owner of both the system and the data. Furthermore, the legal status of a DLT operating in multiple jurisdictions has to be clarified, as it could be difficult to determine under which jurisdiction the DLT operates due to its decentral nature.

While the industry's focus in respect of DLT applications is primarily on the post-trade environment, other specific regulatory challenges may arise around the use of DLT in the pre-trade sphere, for instance when DLT is used for purposes of order matching. Here, compatibility concerns may arise with respect to pre-trade transparency provisions under MiFIR. ESMA has recently pointed out that DLT applications may create additional functions or roles (storing of private keys, coding of smart contracts) not covered by existing regulations.[5]

Lastly, both the regulators and legislators need to be well equipped to deal with emerging technologies, e.g. by forming new multidisciplinary teams with judicial, analytical and information technology skills.

[5] See ESMA (2017) https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

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

This question is most important for market participants to answer, as they can point out more precisely what kind of barriers they face and motivate why certain barriers are unnecessary or unduly complex.

One of the issues that might arise is the 'chain'-responsibility, or the responsibility of the outsourcing institution for the activities of the firm the activity is outsourced to, one of the barriers that is in place for a good reason. We believe that the institution offering a service or product to an end-user is responsible for the full extent of its own products or services, notwithstanding outsourced activities.

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

As stated in our reaction to question 2.10, we believe that the institution offering a service or product to an end-user is responsible for the full extent of its own products or services, notwithstanding outsourced activities. Legal requirements on the outsourcing of activities are currently deemed sufficient, as the CEBS guidelines are currently being updated. We see that improvements can be made in contracting, in particular the inclusion of the right-to-audit, subcontracting and vendor lock-in, as the cloud computing market is increasingly concentrated with a small number of large firms.

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?

There are FinTech startups that specialize in client onboarding solutions and better KYC facilities. This could increase efficiency and result in shorter processes. Also for customers the solutions will be available at all times; online services and products (please see also 2.1).

Another example is that of the potential use of blockchain. For instance, compliance checks whether the execution of a process has been in accordance with relevant laws, eliminating (human) compliance error etc. A smart contract can be programmed to let the imbursement take place if and only if all required conditions have been met and if all legal preconditions have been satisfied in full compliance. As a result, the number of compliance and audit employees van be significantly lowered, resulting in lower operational costs.

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?

The current EU regulatory framework is to a large extent fit to deal with innovation and FinTech solutions. However, both the European and national regulatory frameworks can be adapted when deemed necessary in order to become/remain technology-neutral and activity-based. We believe the momentum is there to start preparing these necessary changes.

While different international policy bodies are studying the impact of FinTech solutions, we believe the Commission should ultimately start working on exchanging best practices and experiences to be able to adapt the current legal frameworks for the large-scale introduction of new techniques such as DLT (while still not mature), AI/Deep learning (e.g. supervision of self learning systems, please see our answer to 1.3), the use of Big Data (e.g. commercial vs. in the clients' interest of, the use of behavioural insights, see also our answer to 1.5), supervision of (personalized) marketing material, competence requirements (machine vs. real person), level playing field in access to infrastructure and the use of RegTech (e.g. for client onboarding).

In the short term, we see the need for regulators and supervisors to focus on the underlying principles and purposes of legislation when applying existing EU and/or Member State legislation, and in addition, to interact and communicate with FinTech companies about these underlying principles and purposes. Where possible, a margin of discretion for innovation should be offered by the regulator/supervisor when applying existing legislation and necessary changes to existing legislation should be signalled to the national and/or EU legislator. This will require an 'accommodating' mindset from both regulators and supervisors and is preferably institutionalized among financial regulators/supervisors. Tools that can help supervisors in dealing with innovations are an InnovationHub and a Regulatory Sandbox. Please see our answer to 3.2 for more details.

3.2. What is the most efficient path for FinTech innovation and uptake in the EU? Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants. If so, at what level?

For consumers and market operators alike, robust supervision and clear regulation remain a vital prerequisite for sustained confidence in established and new financial services or activities. In order to facilitate implementation of FinTech solutions we strongly support interaction with FinTech companies and the 'accommodating application' of legislation by regulators. An open mind to innovation helps to learn more quickly and understand how current developments impact financial services to be able to effectively mitigate risks and adapt legislation. Tools that can help supervisors in dealing with innovations have been introduced in the Netherlands as the InnovationHub and the Regulatory Sandbox.

The 'InnovationHub' with both financial regulators (prudential and market conduct) and the competition authorities on board helps to establish a constructive dialogue with innovative concepts. The hub allows for effective and efficient interaction with FinTech companies (both incumbents, new and in between) regarding all types of questions on the of legislation, and in particular with regard to application of legislation.

The 'regulatory sandbox' allows the Dutch regulators/supervisors to leverage the scope offered by legislation when interpreting the rules on a case by case basis and to review and adapt established policies based on knowledge of new techniques. These initiatives can focus on considering regulatory obligations from a 'rules as intended' instead of 'rules as written' perspective and combine different regulatory perspectives.

Please find more information on these initiatives in the DNB-AFM paper on more room for financial innovation (in English):
https://www.dnb.nl/en/binaries/Discussion%20document%20AFM-DNB%20More%20room%20for%20innovation%20in%20the%20financial%20sector_tcm47-345198.pdf

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 details.

We do not currently see specific regulatory barriers in European legislation that prevent FinTech firms to scale up and provide services across Europe in general. However, differences between Member states in the application of legislation can hamper FinTech companies that operate without an international footprint to provide cross-border services, or due to the national nature of the legislation of certain activities. For example, national supervisors can in practice apply the same European regulatory obligations differently with regard to client onboarding process or to the suitability of board members. In as far as these differences are not justified on the basis of cultural-national differences we support supervisory convergence in these areas and the coordination of regulatory interpretations. We strongly support sharing experiences and interpretation results between national 'regulatory sandboxes' as a way of harmonizing interpretations.

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 yes, 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 strongly support European and national regulatory frameworks to be technology-neutral. Furthermore, legislation should be focused on activities to mitigate the risks linked to the execution of that activity. Introducing general FinTech licensing requirements does not match these principles. There is no basis for treating FinTech activities differently. Rather, the disappearing boundaries between traditional sectors and activities resulting from FinTech solutions call for a more flexible and activity-based approach. Traditional banks become intermediaries in capital, traditional insurers become platform providers or intermediaries in risk. This requires a flexible, activity-based and a cross-sectoral approach to licensing requirements and passporting of activities. Still, robust supervision on passported activities is necessary to preserve trust in the financial system, as we pointed out in our reaction to the consultation of the Mid-Term Review of the Capital Markets Union.[6]

[6] https://www.rijksoverheid.nl/documenten/kamerstukken/2017/03/23/bijlage-consultatiereactie-mid-term-review-actieplan-kapitaalmarktunie (in English)

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? If so, please explain in which areas and how should the Commission intervene.

In line with one of the Commission's core principles – namely proportionality – we support further action on this topic. The European framework should take into account the business model, size, systemic significance, as well as the complexity and cross-border activity of the regulated entities. Areas in which the regulatory framework can be made more proportionate are capital requirements (CRD/CRR), client onboarding and monitoring requirements, and the application of regulatory obligations with regard to partnerships between FinTech companies (between incumbents and new FinTech companies, but also between new FinTech companies and BigTech companies).

Again, we support interaction with FinTech companies and an 'accommodating mindset', e.g. within InnovationHubs or Regulatory Sandboxes, to apply proportionality within the scope offered by European and national legislation.

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? To what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross-border financial transactions?

Although we have been notified that data location regulations constitute potentially hamper cross-border financial transactions, we have thus far not identified specific examples of EU data location regulations being an obstacle to cross-border financial transactions. In the Netherlands, the De Nederlandsche Bank does apply certain data location requirements.[7]

[7] Circular cloud computing 2011/643815 from De Nederlandsche Bank

Issued by the De Nederlandsche Bank on 6 December 2011

See http://www.toezicht.dnb.nl/binaries/50-224828.pdf

The Circular permits cross border use of cloud computing for banking data which is subject to prudential supervision, but requires that it remains subject to effective supervision. This requires a risk based assessment from the outsourcing party, and the conclusion of a contract that allows the supervisor to conduct local audits (or to have these conducted by a third party), an obligation for the cloud provider to provide information to the supervisor upon request, and the right of the outsourcing bank to implement changes in the execution of the services agreement with the cloud provider, including appropriate termination clauses.

A subsequent circular has been issued on the right to examine, indicating a series of cloud providers with whom the supervisor has been able to determine that it will have appropriate examination rights. The list is accessible online.

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

In considering the appropriate regulatory response to technological innovations in the financial sector (FinTech), we believe a number of principles should be consistently taken into account, including the three proposed by the Commission:

- Regulation and supervision should be more **activity-based** as opposed to entity-based: where appropriate similar rules should apply to similar activities, regardless of the entity or sector (collective of entities) performing the activities.
- Regulation, as well as their application, should be **technology-neutral**: equal protections must be afforded to clients and users regardless of the type of technology or methods used. Furthermore, regulations should not inadvertently or unnecessarily pose barriers based on the type of technology or methods used.
- Regulation should be **proportionate**: any regulatory steps in the FinTech sphere must reflect necessary, reasonable and suitable actions to achieve a legitimate aim. This requires a more principle-based (as opposed to a rules-based) approach to regulation and transparency on supervision practices (e.g. in the form guidance).
- Regulation and regulatory interpretations should be **harmonized** across member states: where appropriate similar rules should apply to similar activities, regardless of the country where the activities are performed or the country of the entity. Differences in regulation can be justified (e.g. based on cultural differences) but should not lead to regulatory arbitrage.
- Regulation should be applied with an '**accommodating mindset**' from both regulators and supervisors: when applying legislation supervisors should interact with FinTech companies and focus on the underlying principles and purposes of legislation. We strongly support establishing special teams (such as hubs and sandboxes) in support of FinTech and sharing experiences, best practices and outcomes between national initiatives taken by national authorities.
- Regulation, particularly if designed in a proportionate and principle-based manner, should be complemented by the development of **adequate non-regulatory instruments and remedies**, including civil-law/tort arrangements such as (product) liability mechanisms. Such arrangements yield incentives for market participants to invest in the robustness of their products and to develop certifications for software and related services, thereby providing additional safeguards for clients and end-users.
- Regulation should be developed based on a **horizontal approach**. We strongly support horizontal actions by the Commission, such as the current approach to FinTech.

These principles will help legislators and supervisors strike the right balance between facilitating technological innovation and enhancing the **integrity** (safety and reliability) of these technologies for investors, consumers and the financial system as a whole. These principles are also reflected in our replies to this consultation.

3.8. 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? Would there be merits in pooling expertise in the ESAs?

We support a proactive role for the Commission or the ESAs to stimulate the sharing of best practices between initiatives taken by national authorities in support of FinTech as well as the sharing and publication of outcomes or interpretations of these initiatives (such as special teams, hubs and/or sandboxes to deal with FinTech related questions). We also see merit in using the ESAs to exchange views on how national authorities deal with innovation and FinTech and how to support national authorities in accommodating FinTech.

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 organisations to share practices and discuss regulatory and supervisory concerns? If yes, please specify how these programs should be organised?

We are unaware that any public initiatives in this area are currently deemed necessary. Market participants currently function as bridging partners between public and private sector. Furthermore, the Dutch NCA's have set up an Innovation Hub where market participants and regulators can informally discuss regulatory issues (as pointed out in our reaction to question 3.2).

3.10. Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? If so, who should run the sandbox and what should be its main objective?

We support a proactive role for the Commission or the ESAs to stimulate convergent sandbox initiatives taken by national authorities in support of FinTech and to support the cross-border sharing of best practices and sandbox outcomes, as sandboxes shouldn't lead to regulatory competition between MS. While in theory a harmonized application of European legislation accommodates cross-border activities (i.a. passporting), differences between MS markets, national legislation and application, mean that in practice outcomes can differ across countries, hampering FinTech companies to provide cross-border services. We therefore strongly support the sharing of cross-sectoral experiences and outcomes between national 'regulatory sandboxes'. A future coordinating role by the ESAs on the approaches, including those towards the waiving of requirements stemming from European legislation, could further lead to supervisory convergence and a more common approach.

We do not see merits in establishing a European regulatory sandbox, nor a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border. Providing guidance (which is what regulatory sandbox initiatives mostly do at the moment) and supervision and enforcement should be kept within the same authority, as this authority will often become the competent (Home) authority. National authorities are best equipped to deal with differences in markets and national legislation, and to interact with FinTech companies in such a time-frame that pays due to the often very short time-to-market that FinTech companies rely on. A European sandbox environment adds a another layer of bureaucracy while lacking specific expertise (both national and supervisory) and a mandate/organizational structure for supervision and enforcement. In addition, the current regulatory sandboxes are still in their early phase, operate on an experimental basis, and authorities are still learning from the experiences. The results so far indicate however that these national regulatory sandboxes successfully fulfil a need from FinTech companies to interact closely and on a low-key level.

3.11. What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above? If yes, please specify which measures and why.

-

3.12. Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision? Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

-

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?

We acknowledge the importance of this question and invite market participants and rule-setting bodies to identify the areas mostly suited. We are monitoring, and participating in, discussions on this topic within international bodies, such as the Financial Stability Board, to further explore possibilities in this area.

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? What other specific measures should be taken at EU level?

The European Commission strongly supports the use of OSS, due to the benefits Open Source has for the development of new products and services. We support this goal, but would like to point out that initiatives to promote libraries of open source software should connect to the current initiative of the open source library JoinUp https://joinup.ec.europa.eu/.

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.

FinTech could impact the safety and soundness of incumbent firms in three important ways:

1. the strategic risk of losing business to newcomers such that capital and/or liquidity positions of incumbents are put at risk;
2. increased operational risk because of increasing complexity of business processes and services, as well as the increased reliance on third parties; and
3. increased interdependency as the rise of fintech leads to more and more IT interdependencies between market players (banks, fintech and others) and market infrastructures, which could cause an IT risk event (eg cyber-attack) to escalate into a systemic crisis.

Efficiencies that FinTech could bring to incumbents are i) cost efficiency, ii) greater transparency and reduced information asymmetries, iii) improved risk management, and iv) improved access to and convenience of financial services.

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 and the use of consumer data is already taken up in the Digital Single Market initiative and the aforementioned GDPR, and should be addressed in the appropriate forums. As we already pointed out in our reaction to question 1.5, the Dutch government is preparing a reaction to the initiative report submitted by the member of the Dutch parliament Nijboer. The reaction is expected to be sent to parliament in the third quarter of this year. The initiative report and the cabinet reaction may provide useful insights for the European Commission.

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

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

We believe the current digital identity frameworks to be used with DLT could be improved. One of the working groups within the Dutch National Blockchain Coalition aims develop an identification/authentication framework ready for production use by government and commercially. This initiative is led jointly by the national government's agency for identity registration and issuance of passports/id cards (RvIG) together with Delft University of Technology.

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

The main challenges for using DLT with regard to personal data protection seem to be the question whether DLT offers sufficient protection of personal data, and the difficulties in determining the beneficiary of transactions recorded in a DLT. While these concerns would arise for 'non-proprietary' types of DLT (e.g. Bitcoin), they should not be an issue for proprietary DLTs, owned by (an) institution(s). While technically a DLT is capable of providing various and differential levels of data protection, the design of the DLT application (geographical spread of the ledger's nodes), as well as applicable regulations, can create cost challenges.

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?

Information asymmetry is a barrier to SMEs' access to finance. Providers of financing, being bank or non-bank funding providers, face difficulties to assess the creditworthiness of SMEs, due to limited information being available and costly labour-intensive processes. The OECD stresses the importance of an efficient credit rating infrastructure in its recent report. Credit Rating Agencies, Information systems and technology-based solutions can help to improve risk-profiling by unlocking more information to potential financiers and platforms.

Risk assessments are based on both non-quantitative (viability and trust) and quantitative information, such as assets in place, existing invoices and a payment profile on utility bills, which is scattered and labour-intensive to gather and assess. Therefore, automation and big data analytics could deliver significant results by lowering the costs of credit risk assessments and thus improving access to finance for SMEs by lowering the cost of capital.

The ministry of Economic Affairs of the Netherlands conducted a pilot project ('financing link', FINK) which aimed to improve, standardize and provide access to information on the creditworthiness of SMEs using Standard Business Reporting (SBR) of readily available information. The pilot helped lenders receive (reliable) information on creditworthiness of SMEs. It also helped SMEs receive insight in opportunities and potential interest of various finance providers. The evaluation concluded that the Fink standard can help to explore opportunities. A Fink Roadmap is being implemented and will lead to establishing an open standard for intakes (data needed for contact and insight), leaving the application of the standard and the exchange of data to the market.

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?

Information sharing is a private economic activity that can be supported by public institutions, such as the European Commission, as to aim for interoperability of systems and the availability of information to support the beneficiaries: companies seeking financing and financiers aiming to fund companies. In this respect we expect that PSD2 will fulfill an important role, as it allows for access to the account services, including payment information based credit services. The Commission could monitor the effects of PSD2 and broaden its current action under the action plan consumer financial services to facilitate the exchange of other data between registries to SMEs. Companies could be enabled, for example through standardization and interoperability of (non-transaction) datasets of accounting software, to share also other data with possible financiers.

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?

We acknowledge the importance of this question and invite market participants to identify requirements that may be introduced. We support the principles of cyber resilience by design, an integrated approach for products and channels and end-to-end security as minimum requirement for financial service providers.

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?

The sharing of cyber threat information should be distinguished in reporting (to national authorities) and sharing (with national authorities and) among financial service providers. A major impediment to sharing cyber threat information sharing is classification by law enforcement. Relevant cyber threat information in ongoing investigations should be declassified before it can be shared among other relevant (market) parties.

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)?

With regard to cybersecurity penetration and resilience testing in financial services we strongly support the CPMI Principles for financial market infrastructures. The Netherlands has adopted so-called Red teaming in which ethical cyber attacks based upon integrated threat intelligence are run on a financial institution's network/system/data to discover vulnerabilities. A multiple consent model for testing cyber resilience within international financial institutions could potentially improve willingness to cooperate as well as solve coordination problems stemming from concurrent jurisdictions.

4.10. 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? Are there any regulatory requirements impeding them?

Important focus in the Commission's strategy to enhance development of new FinTech applications is on enabling and securing the use of consumer data. We believe the strategy could even be stronger by looking at the possibilities of enhancing access to data on financial services and products as well. Fintech companies have made us aware that an obstacle to develop new comparison applications is to acquire up to date standardized information on products or services. The developments of new applications integrating consumers' and products and services data could improve market functioning. It would empower consumers and help them overcome certain behavioral heuristics and biases such as choice and information overload. The current regulatory approach of the Commission to information provision is already focused on involvement of behavioral insights to strengthen its impact, for example by generating pdf's with key or summary standardized information. It would be worthwhile exploring how the approach to information provision could be strengthened by integrating opportunities arising from FinTech, in particular by enhancing access to data contained in the information provision by FinTech companies.