Financial Data and Technology Association
c/o The University of Edinburgh
13-15 South College Street
Edinburgh
EH8 9AA

FDATA Europe Response to European Commission's Consultation on Digital Finance Strategy for Europe / Fintech Action Plan June 2020

https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2020-digital-finance-strategy-consultation-document_en.pdf

Forward:	
English	
Trade Union/Other	
Regional	
Financial Data & Technology Association (FDATA)	
Micro	
Transparency Register Number: 250265838689-18	
UK	
Technology Companies (?)	
Activity fields/sectors:	
Public privacy settings:	
Q1: What are the main obstacles to fully reap the opportunities of innovative technologies in the European	FDATA Europe believes that most of the obstacles in the way to fully reaping the benefits of innovative technologies stems from the following four reasons:

financial sector (please mention no more than 4)?	1) Lack of common technical standards, which hinders interoperability across the market. This leads to costly and inefficient variations to interfaces and slows the movement of customer directed data sharing. 2) Lack of a centralised trust framework for authorised, regulated, certified, and compliant actors in the market. By having a centralised directory for the market, ASPSPs can be assured that any TPP requesting access to customer data (at the customer's request and consent) has proper permission, irrespective of the local NCA under which it is authorised. 3) Continued support for bilateral agreements between ASPSPs and TPPs. This hinders consumers' choice in TPPs, and prohibits a fair and level competitive landscape. 4) Secure Customer Authentication implementation being introduced prematurely, before Open/Digital Finance is fully delivered and robustly tested, which results in consumers no longer being able to direct non-payments data which had been previously accessible to TPPs, but which is now blocked. To further point 1 on lack of technical standards, any new Digital Finance Strategy requires a mechanism to neutralise competing interests across the industry that inhibit interoperability. This competing interest - between ASPSPs to control and restrict access to customer owned data via premium/commercial APIs and the fintechs' interest in providing services to end customers not currently offered by ASPSPs - must be addressed. Leaving ASPSPs in charge of technical specifications leads to complexity, lack of interoperability, and is a hindrance to competition. Instead a neutralising mechanism develops technical standards, compulsory adoption of those standards across the industry, pass/fail testing of conformance to such standards, and tight regulation of performance.

	To further point 2, a lack of a centralised trust framework can be extended to include the fragmented approach by member states to common regulatory requirements for universally held compliance requisites. For example, there is no standard for digital identity and KYC/customer due diligence. Having a centralised common standard across all NCAs, including setting up a 'passported' digital identity and KYC/CDD attestation, would facilitate a commonly accepted utility and streamline AML monitoring as well. To further point 3, lack of multilateral agreements between ASPSPs and TPPs is fundamentally anti-competitive, and contrary to the spirit of PSD2. Continuing to permit bilateral agreements will effectively kill a broader digital open finance strategy by limiting the number of TPPs who can viaby compete in the non-payment verticals. Bilateral agreements inhibit that directed data to flow unless there is a pre-existing contract between the data donor and data recipient. Since it is the customer's right to direct their data to any regulated actor of their choosing, any data doner is compelled to share that data to the designated data recipient under PSD2. To continue to support bilateral agreements in terms of access to open banking or open finance APIs, means consumer choice is reduced even further. There should be no need for these agreements - in context of security and confidence, all regulated TPPs should conform to the same standards. To further point 4, the current SCA implementation defeats the political objectives of PSD2 and materially fails to improve security to protect customers. PSD2 policy objectives are materially undermined by the specific drafting contradictions in the RTS. The current application of SCA coupled with the 90 day reauthentication requirement poses considerable hassle and inefficiencies for customers. The customer journey is negatively impacted (often with mandatory redirect to

	ASPSP sites), attrition from TPP services is high thereby diminishing competition, and security is not materially improved. Moreover, any consumer relying on passive refresh notifications to manage their finances are denied the service, as SCA imposes a customer-present access requirement that renders the service impossible to deliver. Regulators should (1) explain the contradiction between PSD2 text and RTS Article 10, and issue an Opinion that ASPSPs are 'not allowed' to require SCA for TPPs within the 90 day period; (2) require that SCA implementations preventing customer-not-present access must immediately remove SCA to enable credential sharing access to resume; (3) allow AISPs to conduct 90 day reauthentication, and SCA to be removed from TPP channels until this is possible.
Q2: What are the key advantages and challenges consumers are facing with the increasing digitalisation of the financial sector (please mention no more than 4)? For each of them, what if any are the initiatives that should be taken at EU level?	1) Customer data right: understanding their right, and having the option to direct their data via any regulated TPP of their choosing; being empowered to share and leverage their data for their economic benefit 2) Customer liability framework: the lack of a robust liability framework is of particular challenge. A comprehensive digital finance strategy also requires a robust customer liability framework, one that makes the customer whole when they suffer loss through no fault of their own; a methodology between firms in allocating blame and cost, which is accurate, fair, and reasonable; and a system to protect regulated market actors from customers making fraudulent claims; and include appropriate levels of cyber security indemnity insurance for all actors.

Q3: Do you agree with the choice of these priority areas?	Yes - in principle 1. ensuring that the EU financial services regulatory framework is technology-neutral and innovation friendly; 2. reaping the opportunities offered by the EU-wide Single Market for digital financial services for consumers and firms; 3. promoting a data-driven financial sector for the benefit of EU consumers and firms; and 4. enhancing the operational resilience of the financial sector.
Q3.1: Please explain your answer to question 3 and specify if you see other areas that would merit further attention from the Commission	Yes, FDATA Europe agrees with the overarching principles. However, we do have concerns about the mechanics of how these principles are enshrined and delivered. The first principle ensuring that the EU financial services regulatory framework is technology-neutral is laudable; however, as we've seen from the disparate and fragmented delivery of open banking across the market, adherence to the principle of strong technical standards has not been met. Allowing the banks to build to highly prescriptive technical specifications means that each bank has built a bespoke, unique API that requires a bespoke, unique interface connection build on the TPP side. This requires TPPs to build hundreds, even thousands, of interfaces. It is costly, redundant, and a barrier to entry for new TPPs trying to crack the market. It also fails the interoperability test. A technology neutral framework requires standardisation. This is even more true as non-payment verticals are opened up to competition. To require bespoke connections for each of vertical exponentially raises costs and resources. It would be a non-starter, and delay true open digital finance delivery by decades. Leaving each bank to build an API at its discretion, albeit to a technical specification, is not neutral. It gives the incumbents complete control over the choice of

	technology. In no other regulated market does the supply side (ASPSPs) have complete control to dictate at a micro level what the demand (TPPs) side must build to connect. The introduction of API technology after PSD2 was put into force shifted the technology build responsibility to include both the supply and demand side. The build burden now put those who desperately needed the data (TPPS) and those fearful of it working too well in case it produced a competitive threat (ASPSPs) in a new position. The only way to neutralise these competing interests is through technical standards and compulsory adoption of these standards across the industry. Pass/fail conformance testing and tight regulation of performance are also necessary. API execution has mostly failed, largely due to a lack of understanding of the fundamental shift in roles and quality control required by a move to APIs. Leaving the supply side in charge of the technical specifications leads to complexity, lack of interoperability, and a hindrance to competition. It is critical that a digital finance strategy take advantage of this lesson, and shift from supply side technical specification builds, to a shared technical standards approach.
Q4: Do you consider the existing EU financial services regulatory framework to be technology neutral and innovation friendly?	No
Q4.1: If not, please provide specific examples of provisions and requirements that are not technologically	The existing EU financial services regulatory framework is not as innovation friendly as it could be. There are several critical provisions that hinder innovation, the two most pressing are:

neutral or hinder innovation:	**Secure Customer Authentication** As currently applied, SCA hinders innovation. Because of the conflicting language in the level 1 PDS2 text, and the level 2 RTS requirements, the current implementation of SCA in the customer journey prohibits both competition and innovation. RTS Article 32(3) requires that ASPSPs not create obstacles to the provision of PIS and AIS services. However, RTS Article 10 language states that PSPs are 'allowed not to apply' SCA (secure customer authentication) in two specific instances. By leaving the choice up to ASPSPs where they put the SCA step in the customer journey, consumers are now being required to be present for the AIS/PIS to access customer data in order to carry out the service. SCA has become an obstacle, one which results in significant customer attrition (FDATA Europe members provided attrition data to the European Commission and EBA in a position paper data 17 April 2020, data showing attrition rates ranging from 13-60%, averaging 35-40% overall). This prohibits innovative business models from going to market, and is anticompetitive. **AML & CDD** The unintentional inclusion of AISPs and PISPs expanded customer due diligence and AML requirements is also hindering innovation. AISPs, as the EBA acknowledged in its consultation (JC 2019 87 CP on draft GL on MLTF risk factors), do not provide payments and are not involved in the payment chain, nor can they conduct financial transactions from within the AISP environment. AML requirements provide limited value at high cost, and are an impediment to both competition and innovation. Any application of AML requirements to AISPs is counterproductive to the purpose of increasing innovation

	and competition. Some AISPs will not be able to continue to operate, and others will not go to market, due to the additional cost layers required by AML/CTF checks and heavier transaction monitoring, thus limiting consumers' access to and use of new disruptive AIS services. Including AIS activity for AML requirements is a drafting oversight, caused by the blanket construal of references to the repealed PSD1 (which did not have the concept of AIS in its definition of 'payment services') as references to PSD2. Any onerous and redundant double-up compliance on an AISP would be counter to the 4MLD objectives of creating a regulatory environment that allows TPPs to grow their business without incurring disproportionate compliance costs, as well as negatively impact competition, customer choice, and convenience. AML requirements for PISPs is also prohibitive of both competition and innovation. Unlike other payment service providers (banks, money remitters, e-money institutions), who come into possession of funds in the provision of their services, PISPs are prohibited from being part of the flow of funds. A PISP is dependent on the customer's bank to actually execute the payment, and move the money from the customers bank to the payee's bank. A PISP does not at any stage of the payment chain hold the user's funds. PISPs are also required to undertake CDD on each end-customer, a requirement inconsistent with PSD2 According to Article 66.3(f), a PISP should not request from the PSU any data other than those necessary to provide the payment initiation service; requiring a full electronic ID verification process violates the minimum information standard set in Article 66.3(f). In the very next clause of Article 66 [3(g)], it goes on to say that a PISP should not use, access or **store** any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer.

	Under AML/CTF requirements, a PISP would need to store this data. Moreover, this requirement also contradicts Article 5(1)(c) of the General Data Protection Regulation (GDPR) on the principle of data minimisation. This obligation also undermines the very principle of "fair competition among all payment service providers" postulated in PDS2: PISPs are subject to stricter requirements in comparison with Card Processors who have a similar business model. PISPs AML checks on end customers are restricted to a manual process. Under PSD2, PISPs are prohibited from using APIs to obtain account information such as name and address. They cannot bypass the manual process. This is not technology nor business model neutral. Obligating PISPs to conduct AML checks on the end customer leads to Open Banking forfeiting its initial goal of encouraging innovation, and providing the customer with competitive choice. **Digital Identity** The lack of digital identity standards is also an impediment to innovation. There is substantial economic friction across EU Financial Services from having so much variation on how identity is established, passed forward, and how authentication takes place. A coordinated and standardised approach to developing a digital identity is critical to the future of digital finance. Letting the market choose the solution puts the customer at risk, because the customer may never have been at the heart of the solution design in the first place and it is likely that we could end with various competing systems in the market. Market led solution adoption puts the onus on the customer to manage more than one type of identity solution, leading to poor customer experience. The lack of

	consistency of these proposed frameworks is problematic. More importantly, there is no interoperability across these varied solutions. Interoperability is key to having a truly competitive financial services marketplace. Requiring any service provider to build multiple interfaces to manage different identity services is not only costly - a cost which is ultimately passed on to the end customer - it is overly complex, inefficient, and creates a barrier to entry for alternative service providers. Critical work is needed to develop identity standards and a more robust consent management model. Without establishing interoperable standards, the integrity of any identity management scheme is compromised. FDATA believes that the organisation best equipped to develop 'open source' technical specifications to enable the rules to be expressed is the Open ID Foundation (OIDF). Their open and collaborative approach would be seen as market sector neutral, and therefore would be a great way to bring the various parties in the EU working on bespoke systems or on sector specific systems into a technological discussion, to ensure that the pathway to add the customer to the 'Trust Framework' is open.
Q5: Do you consider that the current level of consumer protection for the retail financial products and services established by the EU regulatory framework is technology neutral and should be also applied to innovative framework is technology neutral and should be also applied to innovative ones using new technologies, although adapted to the features of these	Yes

products and to the distribution models?	
Q5.1: Please explain your reasoning on your answer to question 5, and where relevant explain the necessary adaptations:	Yes, current consumer protection standards are technology neutral and should be applied to innovative technology business models. Currently lacking is a proper digital finance liability model and system of customer redress. A robust customer liability framework makes the customer whole when they suffer loss through no fault of their own; a methodology between firms in allocating blame and cost, which is accurate, fair, and reasonable; and a system to protect regulated market actors from customers making fraudulent claims; and include appropriate levels of cyber security indemnity insurance for all actors. FDATA Europe sees the following as important inputs into a robust liability model: • Codify the payout for data breach according to a simple formula, and cap the quanta • Upgrade all data recipient institution applications for permission and supervision to bring them into line with the permissions to TPPs (AIS) under PSD2 • Build a single and mandatory Open Finance Customer Redress system, extending from the open banking start point • Compel all actors to use the redress system and to show they are properly trained in how to use it as part of the permission and supervision process • Require all parties to use the Trust Framework (identity/directory) to also identify each other when establishing the system of redress.

	• Build a technical system of ascertaining liability, such as investigating a system of embedded hidden identifiers (such as a watermark) and ensuring forensic audit capability can be required by a Financial Ombudsman Service. • Test the system rigorously and regularly to ensure all actors in the market, including regulators and the Ombudsmen, are properly trained • Set up one Ombudsman for all jurisdictional Financial Services • Require any firm operating in the jurisdiction, regardless of any passporting rules, to be party to the system • Develop a clearer plan for liability and redress in digital finance for the handling of data breach risks to unregulated parties, such as TSPs or any agent or unsupervised party receiving the data from a data recipient institution (DRI). Regulated DRIs should be required to inform customers that if their data is shared outside the controlled domain of Open Finance (data sharing between regulated actors when compelled by the customer) they are still covered under GDPR.
Q6: In your opinion, is the use for financial services of the new technologies listed below limited due to obstacles stemming from the EU financial services regulatory framework or other EU level regulatory requirements that also apply to financial services providers?	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Distributed Ledger Technology (except crypto- assets): 3 Cloud computing - 5 Artificial Intelligence/Machine learning -5

If you see other technologies whose use would be limited in the financial services due to obstacles stemming from the EU financial services legislative framework, please specify and explain:	Internet Of Things (IoT) Biometrics Quantum computing Other
Q6.1 : Please explain your answer to question 6, specify the specific provisions and legislation you are referring to and indicate your views on how it should be addressed:	FDATA sees several challenges relating to the utility of technology solutions given the current regulatory framework. **Cloud computing** The wider adoption of cloud computing may be limited by GDPR and data residency requirements, especially in relation to cross-border and international transactions that include parties who fall outside of the EU. More to the point, there are current problems with multi-cloud interoperability, in particular data portability rights. GDPR establishes data mobility rights, but does not clarify portability rights. Extending the customer data right to include both mobility and portability would address this problem. There is also a lack of data standards (including syntax) that prevent interoperability. A move to address data quality, and establish a Legal Entity Identifier system that would facilitate a data infrastructure system enabling lower data costs and risks, lower reporting burden, and better quality faster data exchange. The lack of technical standardisation across the industry is also a barrier to wider adoption of cloud computing. For any demand side entity, having to build bespoke API interfaces to connect with the supply side is not only

	costly and burdensome, it is inefficient and prevents the speed and scale of interoperability. For any digital finance initiative to work at scale, technical standards are key, as adding additional verticals to the mix (beyond Open Banking payment data), will require additional API builds that are all unique to each financial institution. Connecting, monitoring, and ensuring adequate performance for data sharing and aggregation across all the financial services verticals requires technical standardisation. Anything less would make interoperability impossible. **AI & ML** At the moment, no stringent requirements regarding algorithmic bias/discriminatory outcome exist. There is ample evidence across the market that algorithmic bias exists, and can lead to discriminatory and negative customer outcomes. Also, there is a lack of access to good quality data training sets for new third party provider entrants into the market. This limits their ability to prove business model outcomes, and to providing regulators with assurance that the algorithms used are neutral, beneficial, and meet the 'decision explainability' requirement under GDPR Recital 71. Although the Commission's European Strategy for Data addresses the need for private companies to access quality data sets for algorithm training, and business model validation, the High Impact Project has yet to be established or funded. The current dearth of data sets and available sandbox training opportunities for TPPs entering the market is a pressing matter that may not be able to wait for the delivery of this bigger Data Strategy. One means to immediately address this is for existing regulatory sandboxes to oversee a training data program,

	in collaboration with current certified data safe haven organisations, to allow regulated TPPs to begin using live transactional data training sets. An alternative to live transactional data sets for training, is the use of Synthetic Data sets modeled on actual transactional data. This guarantees anonymity of the personal identifiable information about the data subjects, while offering the utility of actual transactional data. By creating data training sets using synthetic data, privacy laws are met, while ensuring algorithms are trained using qualitatively meaningful and representative data.
Q7: Building on your experience, what are the best ways (regulatory and non-regulatory measures) for the EU to support the uptake of nascent technologies and business models relying on them while also mitigating the risk they may pose? Please specify what are the other ways the EU could support the uptake of nascent technologies and business models relying on them while also mitigating the risks they may pose:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Setting up dedicated observatories to monitor technological and market trends (e.g. EU Blockchain Observatory & Forum; Platform Observatory) - 3 Funding experimentation on certain applications of new technologies in finance (e.g blockchain use cases) - 3 Promoting supervisory innovation hubs and sandboxes - 5 Supporting industry codes of conduct on certain applications of new technologies in finance - 4 Enhancing legal clarity through guidance at EU level for specific technologies and/or use cases -5 Creating bespoke EU regimes adapted to nascent markets, possibly on a temporary basis -4 Re: other support mechanisms/models

	Supporting industry codes of conduct on certain applications of new technology: The market would greatly benefit from access to data training sets that would allow new service providers to develop and validate their products in the context of real or representative data otherwise hard or impractical for them to access before gaining access to customer data themselves. This would also allow access to more representative and better linked data than either banks or new entrants may have had access to on their own. The ever-expanding use of machine-based algorithmic decision making has thrown into sharp relief biases, inequalities and unfairnesses that have always been part of decision-making in the financial services industries (as elsewhere). This has also led to a rise in much clearer thinking about what is meant by terms such as *fairness* and *privacy* in the context of decision-making and shown that all definitions of fairness involve complex trade-offs. The growing use of machine-based algorithmic decision making has resulted in increased scrutiny of biases, inequalities, and unfairness as part of the decision making process in financial services. Having a forum, with appropriate privacy and ethical framework. to test algorithmic models and data for various forms of bias and potential violations of privacy would be very beneficial for all parties in the ecosystem. Allowing a safe and trusted testing environment would encourage financial institutions to bring data and models about which they have concerns up for review and validation, allowing regulators to better establish policy for those evolving models. Having a forum that advises players in the industry on current best practices, offers training for staff, and creates auditing facilities that allow models and data to be securely tested for various forms of bias and potential violations of privacy is incredibly important.

Q8: In which financial services do you expect technology companies which have their main business outside the financial sector (individually or collectively) to gain significant market share in the EU in the five upcoming years? Please specify in which other financial services you expect technology companies to gain significant market share in the EU in the five upcoming years	Rating system – need to check consultation paper 1 (very low market share, below 1%) 2 (low market share) 3 (neutral) 4 (significant market share) 5 (very significant market share, above 25%) NA Intra-European retail payments - 5 Intra-European wholesale payments - 3 Consumer credit provision to households with risk taking - 4 Consumer credit distribution to households with partner institution(s) - 5 Mortgage credit provision to households with risk taking - 3 Mortgage credit distribution to households with partner institution(s) - 3 Credit provision to SMEs with risk taking - 5 Credit distribution to SMEs with partner institution(s) - 5 Credit provision to large corporates with risk taking - 2 Syndicated lending services with risk taking - 2 Risk-taking activities in Life insurance products - 2 Risk-taking activities in Non-life insurance products - 3 Risk-taking activities in pension products - 2 Intermediation / Distribution of life insurance products - 3

	Intermediation / Distribution of non- life insurance products - 4 Intermediation / Distribution of pension products - 4 Other insurance related activities, e.g. claims management - 2 Reinsurance services - 1 Investment products distribution - 3 Asset management - 2 Others
Q8.1: Please explain your answer to question 8 and, if necessary, describe how you expect technology companies to enter and advance in the various financial services markets in the EU Member States	Distribution of financial products will have high uptake, as more platform plays from big tech mean more efficient customer engagement, and consolidated marketplaces. Those big techs with large balance sheets will see profitability in risk taking, so extension of credit products is a natural extension. Many of the big tech companies already taking a foray into financial services are e-commerce giants, and payments processing is already something they do. Both Apple and Google offer wallets for payment options. Amazon launched AmazonGo, a contactless payment option for retail consumers. Apple also recently launched a retail credit card in partnership with Goldman Sachs. Amazon also has a small business lending programme, offers cash deposits, consumer credit and debit cards, and product insurance. Big Tech expansion into payments leads to the nature next step in extending credit, especially for point-of-sale purchasing. By extension, POS credit can also be bundled with non-life insurance products to cover certain large purchases. This is especially relevant for those large e-commerce platforms, like Amazon and Alibaba.

	In fact, Alibaba and Ant Financial's recent establishment of Luxembourg residency shows willingness to expand its financial services offerings into Europe. Same can be said of Japanese e-commerce giant Rakuten, who also has its European headquarters in Luxembourg; they offer the Rakuten Card and financing/lending for small businesses, as well as non-life insurance products. In the UK, the core banking provider FIS is regulated as a PSP, and their planned expansion of payment provisioning and some account servicing is a natural next step. The trend towards Big Tech either offering their own balance sheet financed products, or leveraging a partner ASPSP license is only growing, and will certainly flourish in the next five years.
Q9: Do you see specific financial services areas where the principle of "same activity creating the same risks should be regulated in the same way" is not respected?	Yes. As Big Tech continues its foray into financial services, the ability to acquire and consolidate TPP use cases into a single platform will pose certain competition challenges. The scale and scope of customer acquisition will be fundamentally imbalanced in favour of the big tech giants; access to data will be skewed, as those big tech giants already have more detailed insight into their customers' transactional history. Big Tech is already in a natural monopoly position; competition is either acquired or bulldozed over. The market should not be allowed to be a competition between incumbent ASPSPs and Big Tech, because that is not competition; it does not allow new entrants into a level playing field. Big Tech is a platform play. Experiences from the transition of other industries to a platform model suggest that there are strong oligopolistic, and in some cases even monopolistic, tendencies in platform ecosystems that help early movers consolidate their success in ways that make it extremely difficult to dislodge them. A

	platform model in financial services is likely to only have a handful of players whose success is founded on their ability to control the distribution channels and customer experience. Regulation of Big Tech should be sensitive to the mission PSD2 espouses: of promoting competition, encouraging innovation and improving customer outcome and choice. The principle of regulating 'same activity creating same risk' should not be applied once mass-scale platormificaion is likely to occur. Doing so would not only diminish innovation, but discourage competition, and leave the customer with limited choice, choice determined by the commercial benefits to those platforms alone.
Q9.1:Please explain your answer to question 9 and provide examples if needed:	Although not mentioned in our answer to Question 9, a specific example of need to regulate differently is the expansion of types of credit and credit assessment. Expanded credit availability may need to be regulated differently when alternative data is used for credit assessment. Algorithms and decisioning are different, and adaptive models that consume widely different alternative data may need a different level of scrutiny (regularly updated risk modeling to NCA for approval) But outcome based regulation for risk, rather than specification/input based regulation, should help standardise a 'same activity, same risk' approach to establishing 'same regulation' framework.
Q10: Which prudential and conduct risks do you expect to change with technology companies gaining significant market share in financial services in the EU in the five upcoming years?	Rating system – need to check consultation paper 1 (significant reduction in risks) 2 (reduction in risks) 3 (neutral) 4 (increase in risks) 5 (significant increase in risks)

Please specify which other prudential and conduct risk(s) you expect to change with technology companies gaining significant market share in financial services in the EU in the five upcoming years	Liquidity risk in interbank market (e.g. increased volatility) Liquidity risk for particular credit institutions Liquidity risk for asset management companies Credit risk: household lending Credit risk: SME lending Credit risk: corporate lending Pro-cyclical credit provision Concentration risk for funds collected and invested (e.g. lack of diversification) Concentration risk for holders of funds (e.g. large deposits or investments held in a bank or fund) Undertaken insurance risk in life insurance Undertaken insurance risk in non-life insurance Operational risks for technology companies and platforms Operational risk for incumbent financial service providers Systemic risks (e.g. technology companies and platforms become too big, too interconnected to fail) Money-laundering and terrorism financing risk Other
Q10.1: Please explain your answer to question 10 and, if necessary, please describe how the risks would emerge, decrease or increase with the higher activity of technology	

companies in financial services and which market participants would face these increased risks	
Q11: Which consumer risks do you expect to change when technology companies gain significant market share in financial services in the EU in the five coming years? Please specify which other consumer risk(s) you expect to change when technology companies gain significant market share in financial services in the EU in the five upcoming years:	Rating system – need to check consultation paper 1 (significant reduction in risks) 2 (reduction in risks) 3 (neutral) 4 (increase in risks) 5 (significant increase in risks) Default risk for funds held in non-banks and not protected by Deposit Guarantee Scheme Liquidity risk Misselling of insurance products Misselling of investment products Misselling of credit products Misselling of pension products Inadequate provision of information Inadequate complaint and redress process and management Use/abuse of personal data for financial commercial purposes Discrimination e.g. based on profiles Operational risk e.g. interrupted service, loss of data Other

Q11.1: If necessary, please describe how the risks would emerge, decrease or increase with the higher activity of technology companies in financial services and which market participants would face these increased risks	
Q12: Do you consider that any of the developments referred to in the questions 8 to 11 require adjusting the regulatory approach in the EU (for example by moving to more activity-based regulation, extending the regulatory perimeter to certain entities, adjusting certain parts of the EU single rulebook)?	Yes
Q12.1: Please explain your answer to question 12, elaborating on specific areas and providing specific examples	These risks require an examination of the current liability framework and customer redress system. Unless there is a robust liability framework in place, there is risk that the customer redress process and mechanisms will not adequately meet needs. Also, proper cybersecurity insurance needs to be in place; this would require an evolution of the types of cybersecurity products on offer to the market.

	The other thing that needs to be in place is a proper Trust Framework, ensuring that all actors in the ecosystem are properly accredited, regulated, and meet the required suitable layers of protection for the customer and the customer's data, including: 1. Secure architecture and systems 2. Fit and proper people 3. Privacy policy and compliance arrangements 4. Ongoing security audit and penetration testing 5. Adequate insurance to protect the end customer 6. Mechanism to test the adequacy of the previous points Industry best practices have introduced some central ecosystem components, such as directory functionality. The 'Directory' is essentially a trust framework to establish the identity of regulated actors. The regulatory tests establish suitability of actors. Therefore each actor has assurance that they are only sharing data with an actor that is deemed suitable by the regulator. The liability model also needs certain market level layers, including: 1. Industry best practice legal liability model, described in PSD2, that makes clear that the TPP is responsible to their customers when they are at fault; Requirement for the consent of the customer for both the TPP and ASPSP roles 2. A method for an ASPSP to identify which TPP is connecting on behalf of the customer 3. A requirement for a system of complaint and redress 4. A system of potential sanctions for bad actors Accordingly, an ASPSP (or any other type of data donor institution) should be sharing data under force of law, and should have no further risk if they land the data in the regulated actor of the customer's choice. On that basis, there should be no requirement for a scheme to manage liability, and no requirement for any ASPSP to contract with any TPP for the provision of data.

	There is also no requirement for technical or security due diligence on the TPP by the ASPSP, as all parties in the 'Directory' will be building to the same technical and security standards. This helps create a fair and level playing field, based on clear regulatory decisions, and not based on whether an ASPSP chooses to enter into a commercial contract with a TPP. Dispute management requires adequate identity, traceability, audit capabilities, and the ability to apportion liability. Without the overall liability model being tidied up, firms will be at risk of false claims, and good customers with real faults will be left without redress. A TPP cannot be left offering a customer more than one liability model for a single customer application. Some market harmonisation on dispute management and customer redress would give customers a better outcome. The dispute management system would ideally not exist in the competitive space, in that an average but ubiquitous system would outperform a number of strong offerings. It is just too complicated to have competing offerings. Dispute management between actors and a system that manages customer complaints no matter who in the ecosystem they complain to would seem to be a natural prerequisite. If a customer has one data breach in one application that uses more than one financial set, it would be very difficult for the customer to navigate multiple systems of redress and they should not have to. In a similar vein each financial vertical for data sharing should be connected to a single Ombudsman that is properly resourced and suitably skilled to handle losses connected to financial data. It would be helpful to have some clear formulas for compensation attached to different types of loss to help reduce complexity and ensure adequacy of cover. Dispute management capability should be thoroughly tested by dynamic role playing exercises, to see what would happen in the event of a large volume of customers suddenly making complaints in a lot of different places.

	There is also a role for basic data science, in helping to identify the source of a data breach, in a situation where the customer might not be able to correctly identify the source of the problem. The dispute system should seek to build some monitoring capability to provide a heat map that correlates emerging issues.
Q13: Building on your experience, what are the main challenges authorities are facing while supervising innovative/digital players in finance and how should they be addressed? Please explain your reasoning and provide examples for each sector you are referring to (e.g. banking, insurance, pension, capital markets):	One critical challenge is establishing the key principle of customer directed data, and clarifying its definition. The customer's ability to enforce control of their financial data and how it might be used may need the fundamental protection of the law. PSD2 creates data mobility for payments data. GDPR creates some right of universal portability. One helpful definition to clarify the difference is that 'portability' enables the data subject to get data back to themselves in a machine readable format, whereas 'mobility' enables the data subject to compel through explicit consent one regulated actor to share specified data with another regulated actor. In addition, creating clarity in the liability model and who would pay in certain situations, might make it easier for the regulatory interpretations to develop more easily. The law is not a great place to assert technical requirements nor develop lower level policy surrounding implementation. There needs to be sufficient head room for regulators and leaders from the commercial space to solve problems and make adjustments to fulfil the policy objectives intended. It helps to have a really clear statement of the principles and overarching objectives and for the regulatory leadership to engage in understanding the policy requirements and consult with market participants. Outcomes and standard based regulation is superior to prescriptive regulation. To ensure continuity in the market, any new solution which interrupts the 'Live Market' of firms operating in this domain will need to be blocked from going live until the Live Market issues are resolved. 1. There must be alignment across delivery timetables and clear management of any

	inconsistencies that might create end customer and marketplace problems for existing services 2. There must be an application and approval process for AISPs; to protect the market, there must be a strong method for assessing and verifying AISP 'fitness' a. This must include technical standards, security configuration, data privacy, and various frequent audits against permissioned standards b. There must also be a test of whether the application has adequate risk based liability insurance cover to be accepted into the market 3. There needs to be a process to remove or suspend an AISP from the market if it is not meeting the obligations of its permission or if it has suffered some security or data breach 4. There must be a method of sanction against nefarious actors who seek to operate without a regulated TPP status 5. There is a need to support a digital certificate issuing capability to easily determine actors' regulated status 6. Suitability of applicants should track to the PSD2 text, both to avoid inconsistencies and to gather evidence of changes required for a different process By following this methodology, all verticals included in digital finance can be monitored and assessed for risk in a standardised fashion. This simplifies the approach for adding in new verticals, provides the same oversight for each actor, and ensures the liability model is consistent and easier to manage. It also provides more clarity to the end-customer on how to initiate redress if a problem occurs.
Q14: According to you, which initiatives could be put in place at EU level to enhance this multi-disciplinary cooperation between	The primary challenge is coordinating the individual member state NCAs to fully align with one another and the EU level regulatory framework. Having different technical specifications acceptable across the member states leads to inconsistencies, lack of

authorities? Please explain your reasoning and provide examples if needed:	interoperability, and more costly integration builds (costs which are ultimately passed on to the end-customer). Moving from highly prescriptive technical regulation to an outcome and standards based approach for non-payment verticals is critical. There will be a need to apply this same technical standards approach to payments in order to pave the way for digital finance. Having separate, unconnected, management of approved and certified regulated actors (a directory of licensed, regulated actors registered in each/multiple member states) is also untenable. Rolling in new verticals across a disconnected system increases the complexity; instead, creating a single view of permissioned actors, with a standardised management of that view, allows for a 'source of truth' approach. This single register (or 'Directory') of TPPs means all ASPSPs can easily identify approved actors whom customers have provided consent to provide services. This 'Directory' can be expanded to incorporate any additional vertical (pension, investment, savings, credit, etc.), and can be pan-European inclusive. Any actor licensed by the local NCA can be automatically added to the EU register, if the local NCA license is pasportable.
Q15: According to you, and in addition to the issues addressed in questions 16 to 25 below, do you see other obstacles to a Single Market for digital financial services and how should they be addressed?	Lack of technical standards is the single most frustrating obstacle to a single market for digital services. Again, FDATA Europe members believe that adherence to the principle of strong technical standards has not been met, due to the disperate and fragmented delivery of open banking across the market. There is a fundamental need for standardisation in order to ensure a technology neutral, interoperable framework for digital finance.

	For Digital Finance to be successful, ASPSPs cannot be left in control to dictate what TPPs must build to connect. The only way to neutralise competing interests is through technical standards and compulsory adoption of these standards across the industry, along with pass/fail conformance testing and tight regulation of performance (which, as a technology problem, can be managed with a technology solution). Leaving ASPSPs in charge of the technical specifications is not sustainable for a digital finance strategy. It leads to undue complexity, lack of interoperability, and a barrier to competition. A shared technical standards approach across all digital finance verticals - *including payments* - is adopted. There is tremendous value in establishing technical standards, from both a technology and implementation perspective, including: • Reduced complexity and risk • Protecting customers and all market participants in a cohesive ecosystem by reducing risks and creating certainty that TPPs can offer a complete service to all their customers • Reducing the building, operational, and maintenance costs for TPPs and APSPSs • Reducing security costs by significantly slimlining penetration testing and audit requirements • Enabling investment in customer-facing innovation, rather than tying up resources to maintain plumbing • Making it easier for smaller firms (including smaller banks and TPPs) to participate, improving fairness and competition • Simplifying the ability to trace issues, assess fault, and allocate loss, which makes it easier to establish a liability model and better enables cyber risk insurers to assess threats and perform during the underwriting and handling of claims

	• Creating clarity for ASPSPs, TPPs, and regulators by providing clear, consistent guidelines for compliance (and simplifying the process of adjusting market standards as time progresses) • Reducing barriers to innovation, as creating consistency in data output simplifies the development process for all actors • Enables more rapid growth and better sharing of best practices across jurisdictions Another obstacle to a digital financial services single market is the lack of certain common utilities, in this case both identity and portable eKYC. Adopting a pan-European identity scheme may not be feasible, however, encouraging member states to build a framework that has interoperable standards and regulated providers would facilitate an ecosystem that allows the customer to direct their identity and associated data to the actor/provider of their choice. This also streamlines the process to validate identity along each actor in the service value chain. Identity needs to be interoperable, and put the customer at the centre of directing and authenticating their data. The system requires built-in-trust, and should be easily relied upon by all parties that it meets a baseline standard set by law makers. The same can be said for eKYC. Current practice is for each ASPSP to set up their individual checklist to validate that KYC meets their own internal risk appetite and governance process. There are no two ASPSPs performing KYC in the exact same way. However, there are elements of KYC common to each and every institution. By creating an eKYC standard that encompasses these core elements, regulators can expedite the KYC process. Additional, or enhanced customer due diligence, is left to the institutions who have a higher threshold or internal governance requirement; but the regulatory baseline will

	be met and acceptable across all institutions and actors in the market. Since KYC is a regulatory requirement, a regulatory solution can create a customer-centric, standardised, portable attestation of KYC that can be accepted across all ASPSPs in Europe; regulation can create an interoperable utility solution to eKYC to facilitate a digital finance strategy. By turning KYC into a utility, compliance costs and complexity are reduced; all customers experience a similar journey and have clear expectations as to what the process entails; supervision is simplified; and all actors can be assured that by accepting another institution's eKYC that regulatory standards have been met.
Q16: What should be done at EU level to facilitate interoperable cross-border solutions for digital on-boarding? Please specify what else should be done at EU level to facilitate interoperable cross-border solutions for digital on-boarding:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Harmonise rules governing customer due diligence requirements in the Anti-Money Laundering legislation - 5 Harmonise rules governing the acceptable use of remote identification technologies and services in the Anti-Money Laundering legislation - 5 Broaden access for obliged entities to publicly held information (public databases and registers) to enable verification of customer identities - 4 Provide further guidance or standards in support of the customer due diligence process (e.g. detailed ID elements, eligible trusted sources; risk assessment of remote identification technologies) - 4

	Facilitate the development of digital on-boarding processes, which build on the e-IDAS Regulation - 3 Facilitate cooperation between public authorities and private sector digital identity solution providers - 3 Integrate KYC attributes into e- IDAS in order to enable on- boarding through trusted digital identities - 4 Other - NA FDATA Europe would like to point out that market led identity solution adoption puts the onus on the customer to manage multiple identity solutions which leads to poor customer experience. More importantly, there is no interoperability across these varied solutions. Without interoperable identity standards, the integrity of any identity management scheme is compromised. FDATA Europe believes the organisation best equipped to develop 'open source' technical specifications to enable EU identity rules to be expressed is the OpenID Foundation. Their open and collaborative approach would be seen as market sector neutral, and therefore would be a great way to bring the various parties in the EU working on bespoke systems or on sector specific systems into a technological discussion, to ensure that the pathway to add the customer to the 'Trust Framework' is open. FDATA would also like to point out the importance of harmonising rules for AML and CDD across Europe. We also **strongly believe that AISPs should be carved out from any application of AML requirements in the EU.** AML requirements to AISPs would not serve the purpose for which they were intended, and be disproportionate to the risk (there is none) of any money laundering or terrorist financing occurring through AISP platforms. It would be onerous and redundant to apply AML requirements to AISPs, and have a negative impact

	on the innovation and competition that PSD2 and Open Banking were intended to create. **Should carving out AISP from the application of AML requirements not be possible, any application of the requirements to AISPs (and PISPs) should be limited to the requirement to undertake a risk assessment of their activities**, taking into account the nature of the activities the AISP/PISP is partaking in and the likelihood of AISP/PISP services being used to aid the flow of illicit finance. If, based on the outcome of that risk assessment, the AISP/PISP believes that there is negligible risk of money laundering occurring, it is our view that it should not be subject to any further AML requirements. In the AISP use case, the AISP can only access transaction information from an ASPSP if the payment service user provides its consent and authenticates with its bank in order to allow the AISP to access their payment account. In this scenario, the payment service user will already have undergone CDD at the banks' end, and any further CDD requirement on AISPs would be onerous and unnecessary. Given that PISPs do not come into possession of funds, or execute transactions themselves, (but rather rely on banks to do this), it would be duplicative for PISPs to monitor and report transactions. It may be possible for an AISP/PISP to rely on CDD measures conducted by the bank but this would not relieve the AISP/PISP of responsibility for the CDD obligation. Performance of CDD should be the sole responsibility of the bank and an AISP/PISP should not have any liability for it.
Q17: What should be done at EU level to	Rating system – need to check consultation paper

facilitate reliance by financial institutions on digital identities gathered by third parties (including by other financial institutions) and data re-use/portability? Please specify what else could be done at EU level to facilitate reliance by financial institutions on digital identities gathered by third parties (including by other financial institutions) and data re-use/portability:	1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Make the rules on third party reliance in the Anti-Money Laundering legislation more specific - 4 Provide further guidance relating to reliance on third parties for carrying out identification and verification through digital means, including on issues relating to liability - 4 Promote re-use of digital identities collected for customer due diligence purposes in accordance with data protection rules - 5 Promote a universally accepted public electronic identity - 5 Define the provision of digital identities as a new private sector trust service under the supervisory regime of the eIDAS Regulation - 4 Other
Q18: Should one consider going beyond customer identification and develop Digital Financial Identities to facilitate switching and easier access for customers to specific financial services? Should such Digital Financial Identities be usable and recognised throughout the EU?	Yes, digital financial identities (DFIs) have merit, as long as they are framed out by the consumer data right. DFIs should be mobile and portable. However, who manages them, who has custodianship over them, and how they are directed (at the customer's discretion) need to be clearly established. The composition of DFIs should be standardised, and if there is to be a competitive (private sector) identity provider, then customer experience and custodianship/management need to be the competitive aspect, not the composition of the identity. Interoperability requires standards.

Which data, where appropriate and in accordance with data protection rules, should be part of such a Digital Financial Identity, in addition to the data already required in the context of the anti-money laundering measures (e.g. data for suitability test for investment services; data for creditworthiness assessment; other data)? Please explain your reasoning and also provide examples for each case you would find relevant.	An identity trust framework is also required, establishing a 'Directory' of trusted, regulated, licensed ID providers would be appropriate. There also needs to be a liability framework and customer redress model if a new private sector ID is offered. Counterpoint to this is ID as a utility - and managed at the member state level as a utility. This requires contemplation of the costs of oversight and administration of both a 'private sector' model and state utility model. A number of questions follow that ought to be considered: Which is most efficient? Which has lowest operational costs? Which allows standards to be enforced most easily? What data points/attributes need to be included in DFI? Should there be a tiered DFI?: • Baseline (current account & payments) • Tier 1 (baseline + credit risk) • Tier 2 (Tier 1 + suitability) How is that managed? How is insurance risk assessed for baseline + tiers? How much is the customer charged for that custodianship? How is the funding model split between demand (ASPSP) for identity in order to sell services/products, vs. end-customer who wants to acquire the service? Could it be net neutral in terms of pricing; but then cost of identity custodianship is also theoretically net neutral, so who shoulders the cost? In a private sector model, the ID custodian has to bill someone for the service; in a utility model, there's a sort of 'universal service fee' approach where the utility is subsidised by a small fee to both demand and supply side. Whichever system is selected, it must be designed with the consumer at the heart of it, include mobility and portability, and be built on the principles of standardisation.

Q19: Would a further increased mandatory use of identifiers such as Legal Entity Identifier (LEI), Unique Transaction Identifier (UTI) and Unique Product Identifier (UPI) facilitate digital and/or automated processes in financial services? If yes, in which framework(s) is there the biggest potential for efficiency gains?	
Q20: In your opinion (and where applicable, based on your experience), what is the main benefit of a supervisor implementing (a) an innovation hub or (b) a regulatory sandbox as defined above?	A number of FDATA Europe members have been through the regulatory sandbox experience, and have found it to be of true value. As such, we see a number of benefits from having a more and a more orchestrated approach to member state regulatory sandboxes: • the ability to align compliance and regulation with the rapid growth in fintech business models without overly regulating, and without compromising customer security • the ability for regulators to develop more appropriate policies through greater visibility into new innovations • the ability to provide better customer protection, because products/services are tested in controlled environment before official rollout, and because regulatory bodies are able to implement more focused policies • the ability for banks to have more confidence in an entity's ability to comply with regulation while still being able to develop innovative products and services

	• the ability to reduce the time-to-market at potentially lower costs innovative products and services that benefit the end customer • the ability for innovative fintechs to better attract investment by proving compliance and market readiness All of these benefits are predicated on the sandbox following best practices. For Europe, we recommend looking to the UK's FCA as a best practice model.
Q21: In your opinion, how could the relevant EU authorities enhance coordination among different schemes in the EU? Please specify how else could the relevant EU authorities enhance coordination among different schemes in the EU:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Promote convergence among national authorities in setting up innovation hubs and sandboxes, through additional best practices or guidelines - 5 Facilitate the possibility for firms to test new products and activities for marketing in several Member States ("cross border testing") - 5 Raise awareness among industry stakeholders - 3 Ensure closer coordination with authorities beyond the financial sector (e.g. data and consumer protection authorities) - 4 Promote the establishment of innovation hubs or sandboxes with a specific focus (e.g. a specific technology like Blockchain or a specific purpose like sustainable finance) -3 Other

Q21.1: If necessary, please explain your reasoning and also provide examples for each case you would find relevant:	
Q22: In the EU, regulated financial services providers can scale up across the Single Market thanks to adequate licenses and passporting rights. Do you see the need to extend the existing EU licenses passporting rights to further areas (e.g. lending) in order to support the uptake of digital finance in the EU?	Yes, existing passports will need to be extended to other financial service verticals if digital finance is to be adopted. This leverages the single EU rulebook, thereby allowing authorised, regulated, and supervised firms of any EU or EEA state to operate with minimal additional authorisation, allowing customers across the EU to benefit from innovative products and services in a timely and competitive manner. Passport licensing helps promote competition, innovation, and customer choice.
Q23: In your opinion, are EU level initiatives needed to avoid fragmentation in the Single Market caused by diverging national measures on ensuring non-discriminatory access to relevant technical infrastructures supporting financial services? Please elaborate on the types of financial services and technical infrastructures where this would be relevant and on the	Yes, mechanisms need to be put into place to ensure any non-discriminatory access to relevant technical infrastructures for digital finance to be delivered. For example, User Managed Access, including person-to-person/entity-to-entity consent sharing, will be one of the problems to be solved in the digital finance economy. Currently, user managed access flows from person to company, using OpenID Connect as the authentication standard. However, when person-to-person data sharing is required, developing a process to authenticate Push User Managed Access must be defined. In P2P data sharing, both parties must be authenticated by a central authority. It is this authorisation service that permits access to the data.

type of potential EU initiatives you would consider relevant and helpful:	The underlying infrastructure to do this is missing, including the lack of interoperable national identity schemes, or a single EU identity standard. Some member states do not even have a national digital ID scheme. It also must be noted that whoever builds the infrastructure for a centralised authorisation utility will end up dominating the market. It also requires addressing the balance between the technical complexity of such a system and the need for smooth customer experience, which in of itself has levels of complexity. Therefore the following questions about this infrastructure need to be addressed: • Should this be considered a shared service? • Should this be considered a utility service? • Should this be left to market players to run? • Should this be government or regulator run/operated? • Should this be run by a Trustee? • Should this be a consortium or industry member owned cooperative (like SWIFT) It must be acknowledged that pricing, access, and the level of competition will be determined by whoever builds and controls the infrastructure. It is almost certain an initiative to address a centralised authorisation utility for consent management will be required in order to deliver digital finance in the EU.
Q24: In your opinion, what should be done at EU level to achieve improved financial education and literacy in the digital context? Please specify what else should be done at EU	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant)

level to achieve improved financial education and literacy in the digital context:	Ensure more affordable access at EU level to financial data for consumers and retail investors Encourage supervisors to set up hubs focussed on guiding consumers in the digital world Organise pan-European campaigns and advisory hubs focusing on digitalisation to raise awareness among consumers Collect best practices Promote digital financial services to address financial inclusion Introduce rules related to financial education comparable to Article 6 of the Mortgage Credit Directive, with a stronger focus on digitalisation, in other EU financial regulation proposals Other
Q25: If you consider that initiatives aiming to enhance financial education and literacy are insufficient to protect consumers in the digital context, which additional measures would you recommend?	
Q26: In the recent communication "A European strategy for data", the Commission is proposing measures aiming to make more data available for use in	The core principle of digital finance (or open finance) is reducing information asymmetries. As such, all consumers should have access to digital finance. Every account holder (individuals, SMEs, and large corporates - should be able to direct that data be shared.

the economy and society, while keeping those who generate the data in control. According to you, and in addition to the issues addressed in questions 27 to 46 below, do you see other measures needed to promote a well-regulated data driven financial sector in the EU and to further develop a common European data space for finance?	First and foremost, the customer data right needs to include both mobility *and* portability. The right should be based on the principle of reciprocity: any firm accredited to receive data must also respond to requests from their own customers to share data. All participants should be obligated to comply with a customer's explicit direction to share data. A digital finance system in which all eligible entities participate - as both data holders and data recipients - is fully fairer, more effective, and competitively dynamic. The principle of reciprocity also means that an accredited data recipient in a designated sector (or financial vertical) should also be obliged to provide equivalent data in an equivalent format, in response to a direction from a customer. As a precursor to a larger data-driven economy, the principle of reciprocity should apply across all sectors (energy and telecommunications, for example). A customer should be able to request data from a data holder in one sector (such as energy), that can be provided to a data recipient in another sector (such as banking) if all of the security, technology, and accreditation requirements are met. The liability framework should be based on fault, rather than being based on the initial customer relationship. The model established in PSD2 should serve as a template for a wider digital finance liability framework. FDATA's member hold the following principles, and believe them to be critical to the success of Open Banking, and a fuller digital financial strategy: **Customer Data Right**: The customer has a right to direct the sharing of their data with any regulated actor of their choosing. This includes both data mobility and portability.

	Consent: The customer must have complete control over the granting and retracting of data sharing, within a standardised, easy to understand process. The authorisation service infrastructure to manage this must be market neutral, and not built or run by a private commercial entity. **Data Access Rights**: As with PSD2, the development of Open Finance should start by securing the right for consumers to access their wider set of financial data across all verticals via third-parties, granting third-parties that access via the consent mechanism. **Testing Before Rules**: Authorities should focus energies on bringing data holders and third-parties together to work out how to facilitate the access right, and to identify where the access right can have the most value for consumers, before creating rules. **API Performance & Conformance**: All means should be taken to enforce the performance standards established by law, with transparent action against those parties who effectively lock customers out of open banking for extended periods through API failure. **Non-Payment Data**: Action must be taken to enable access to non-payment accounts via API; since non-payment accounts are not covered by PSD2, rules in this space would not be maximum harmonizing, and lead to more complexity as other financial verticals are rolled into Open Finance. **Standards & Governance**: An entity charged with the maintenance of open data standards, independent of bank control, should be the steward of Open Finance delivery and implementation; Independent oversight of API provision and performance is required for the benefit of the wider open banking ecosystem.
Q27: Considering the potential that the use of	Rating system – need to check consultation paper

publicly available data brings in finance, in which areas would you see the need to facilitate integrated access to these data in the EU? Please specify in which other area(s) you would see the need to facilitate integrated access to these data in the EU:	1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Financial reporting data from listed companies Non-financial reporting data from listed companies SME data Prudential disclosure stemming from financial services legislation Securities market disclosure Disclosure regarding retail investment products Other
Q28: In your opinion, what would be needed to make these easily usable across the EU? Please specify what else would be needed to make these data easily usable across the EU:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Standardised (e.g. XML) and machine-readable format Further development of the European Financial Transparency Gateway, federating existing public databases with a Single EU access point Application Programming Interfaces to access databases - 5 Public EU databases Other

Q29: In your opinion, under what conditions would consumers favour sharing their data relevant to financial services with other financial services providers in order to get better offers for financial products and services?	FDATA members already deliver a number of services to the market leveraging open banking data; foundational to offering these services are the following conditions: • clear, transparent terms and conditions • clarity on what the consented data share will be used for, and for what timeframe • clear security measures • registration/listing in the trust framework (along with all licensed and regulated actors in the ecosystem) • confirmation that all actors in the value chain are regulated, accredited, and licensed • clear and simple customer redress model • clear and effective liability model • least amount of friction to be onboarded or enrolled in the service • least amount of friction in the initial SCA and consent sharing journey • ease of switching services when better deals become available • ease of automating services, with least amount of interruption of service (including re-authorisation journey)
Q30: In your opinion, what could be the main benefits of implementing an open finance policy in the EU? If you see other benefits of implementing an open finance policy in the EU, please specify and explain:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) More innovative and convenient services for consumers/investors, e.g. aggregators, comparison, switching tools - 5 Cheaper traditional services for consumers/investors - 5

	Efficiencies for the industry by making processes more automated (e.g. suitability test for investment services) - 5 Business opportunities for new entrants in the financial industry - 5 New opportunities for incumbent financial services firms, including through partnerships with innovative start-ups - 5 Easier access to bigger sets of data, hence facilitating development of data dependent services - 4 Enhanced access to European capital markets for retail investors - 3 Enhanced access to credit for small businesses - 5 Other (Fuller financial inclusion. Access to insurance is part of the definition of financial inclusion. Additional verticals, insurance being one, added into digital finance means more risk coverage for the average consumer. Also, lower barriers to accessing credit. By leveraging alternative data, and easily obtained transactional data beyond 90 days, thin-file consumers are more likely to meet affordability measures, as well as establish more accurate credit risk scores. This expands the number of consumers who meet credit worthiness benchmarks, resulting in a wider pool of credit eligible consumers.)
Q31: In your opinion, what could be the main risks of implementing an open finance policy in the EU?	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant)

If you see other risks of implementing an open finance policy in the EU, please specify and explain:	Privacy issues / security of personal data - 4 Financial exclusion - 3 Poor consumer outcomes (e.g. unfair pricing strategies) - 4 Misuse of consumers' financial data - 3 Business confidentiality issues - 3 Increased cyber risks - 3 Lack of level playing field in terms of access to data across financial sector activities - 5 Other The EBA's Opinion on TPP Obstacles (90 Day Reauthentication)
Q32: In your opinion, what safeguards would be necessary to mitigate these risks?	FDATA believes that the following are critical safeguards that would mitigate the risks of delivering open/digital finance: • Standardised security protocols (SCA doesn't enhance things as currently implemented) • Addition of digital identity to mitigate risk of financial inclusion • A mechanism that mitigates the 'privacy premium' for those customers who do not allow the same level of data access; excluding customer who do not agree to data sharing, or penalising them with less favourable deals • Creating an execution-only environment could lead to poor outcomes for customers who would have been better taking advice; there is a need to find a balance between advice & execution

	• Auto-switching could lead to less consumer engagement and/or focus price over other suitability factors (also bleeds into execution-only vs. advice risk) • Clarity & transparency of services, fees & pricing as part of t&c/consent model to help mitigate poor consumer outcomes • Robust customer redress model to mitigate poor consumer outcomes • Clear liability framework, and additional cyber risk insurance product choice (to address increased cyber risks) • Consumer data right and principle of reciprocity should level the playing field in terms of access to data across financial sector activities • A mandatory system of reciprocity over bilateral agreements to access data, as the data consented to be shared is owned and directed by the consumer, not the data custodian nor the data recipient
Q33: In your opinion, for which specific financial products would an open finance policy offer more benefits and opportunities? If you see other financial products that would benefit of an open finance policy, please specify and explain:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Savings accounts - 5 Consumer credit - 5 SME credit - 5 Mortgages - 5 Retail investment products (e. g. securities accounts) - 5 Non-life insurance products (e.g. motor, home...) - 5

	Life insurance products - 5 Pension products - 5 Other (all payments data, including credit cards and PSD2 scope) Consumer credit: secured & unsecured loans, overdraft Savings accounts: also includes tax efficient savings These verticals allow for the expansion of intelligent finance, pushing new business models to market that focus on improving financial health, and optimisation of the economic value of consumer money.
Q33.1: Please explain your answer to question 33 and give examples for each category:	Use cases: **Savings accounts:** Automated savings, including nudges for fixed or recommended sums, which can grow over time. **Consumer credit:** Digitised bank data can resolve a raft of issues within the underwriting, credit risk, and fraud decisioning. It improves the time to execute the application (digital onboarding), risk assessment, decision, underwriting, and distribution of credit, allowing for timely and more accurate risk based pricing for credit. Bank data can offer the insights needed to make a genuinely informed decision, and can dramatically reduce fraud. Transactional data also provides insight into risk for thin-file customers, allowing for more fair access to credit for those who have been previously excluded from the credit system. **SME credit:**

	Similar to the consumer credit use case, the use of bank data combined with cloud accounting services data, improves fair access to credit for SMEs. Again all the advantages detailed above are applied. Automating data access around invoicing, cash positioning, receivables and payables, allows for a better credit fit, be it invoice or asset financing. It also expands the number of SMEs who previously fall outside of the risk appetite for traditional lending, expanding the number of truly credit worthy SMEs. **Mortgages:** Much of the information that is required by mortgage assessors and brokers can be gleaned from a bank statement. This is information such as salary, debts, creditworthiness and affordability. Information required by a mortgage assessor can be categorised and classified, and visually presented, offering a rich and detailed picture of the applicant. Bank data also holds substantial advantages over credit reference agency (CRA) data, on which mortgage decisions are mainly based. CRA data is also of limited use for thin-file applicants. Bank data can evidence what a credit score cannot. For example, it could show that a young person has successfully paid rent for the last five years, at a rate higher than the mortgage that they are applying for and is therefore, a candidate for a mortgage. With bank data, a far more detailed and nuanced understanding of an applicant can be built. This information can be layered on top of CRA data to give a fuller picture. Critically, bank data is based on current information, not historical, backwards CRA records. **Retail investment products:** • Help consumers better understand their investments and consider whether they continue to meet their needs by providing up-to-date

	information on costs, tax treatment, performance, risk, and other factors (e.g. asset mix, fees, etc.) • Provide an aggregated view of investments • Help consumers manage investments (easier buying and selling of investments, or moving investments between products and providers) increasing competition and leading to potential for higher returns and/or lower costs • Provide better information about or advise on alternative products or tax-advantage wrappers • Provide an easier and quicker fact-find to reduce investment advice and investing costs • Facilitate switching through platforms to lower investment costs • Open Finance also enables the growth of alternative investment opportunities. **Life & Non-life insurance products:** • Better cyber risk coverage, expanded to include consumers • Better risk based pricing • Reduction of fraud • Reduction of claims handling costs, including improved reconciliation and reimbursement processing • Improved personalised advice • Expanded service offerings, including current accounts • Better deal engines, including better risk profiling, which leads to better pricing on insurance products **Pension products:** • Better understanding of how savings behaviour can affect retirement income (e.g.. mapping projected potential annuity income against personal expenditure rates) to aid informed decisions about savings levels • Tools to help consumers manage pension investments, increasing competition and leading to

	potential for higher returns and or lower costs through: ○ Provision of better information about alternative products or tax advantage wrappers ○ Easier buying or selling of investments, or moving investments between products and providers • Easier and quicker fact-find has potential to reduce costs of advice on investments or costs of investing • Seeing pension pots alongside non-pension savings or assets in one place to ensure consumers can consider together all the assets they can use to fund their retirement • Services offering transfers could make consolidation of pension pots easier, with the potential to also reduce overall charges • Improved view of over all financial circumstances can improve decisions about types of products (annuities vs. drawdown) • Improved search and comparison of specific retirement products
Q34: What specific data (personal and non-personal) would you find most relevant when developing open finance services based on customer consent? To what extent would you also consider relevant data generated by other services or products (energy, retail, transport, social media, e-commerce, etc.) to the extent they are relevant to financial	We believe the following types of data should be considered relevant for open finance: <u>Energy & telecommunications:</u> For switching services, to find a better utility rate to optimise pricing <u>Transport & Travel:</u> known traveler digital identity facilitates KYC and customer onboarding, as well as authentication methods; discounted or credit offerings for point of sale financing; seamless travel insurance offerings <u>Real estate:</u> accomodation matching, affordability, rental & mortgage insurance, subsidising of down payment

services and customers consent to their use? Please explain your reasoning and provide the example per sector:	Wage transparency: enhanced credit risk assessment for both credit and insurance E-commerce transactions (to the degree the consumer is comfortable sharing, with a clear articulation of value for that share): better categorisation tracking for budgeting, and personal finance management; discounting or credit offerings at point of sale Health and movement data: better risk pricing for health insurance products
Q35: Which elements should be considered to implement an open finance policy? Please specify what other element(s) should be considered to implement an open finance policy:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) Standardisation of data, data formats - 5 Clarity on the entities covered, including potential thresholds - 5 Clarity on the way data can be technically accessed including whether data is shared in real- time (e.g. standardised APIs) -5 Clarity on how to ensure full compliance with GDPR and e- Privacy Directive requirements and need to ensure that data subjects remain in full control of their personal data - 5 Clarity on the terms and conditions under which data can be shared between financial services providers (e. g. fees) - 5 Interoperability across sectors - 5 Clarity on the way data shared will be used - 5

	Introduction of mandatory data sharing beyond PSD2 in the framework of EU regulatory regime - 5 If mandatory data sharing is considered, making data available free of cost for the recipient - 5 Other The principle of reciprocity is essential for open finance to work. This means that anytime the consumer compels th data to be shared, the data recipient receives the data free of charge. Any data in scope of a digital finance initiative must not be relegated to a bilateral agreement between financial service providers, be they ASPSPs or TPPs. To require any sort of bilateral agreement in order to access data is to relegate the market closed, rather than open.
Q36: Do you/does your firm already deploy AI based services in a production environment in the EU?	
Q36.1: If you/your firm do/does already deploy AI based services in a production environment in the EU, please specify for which applications?:	
Q37: Do you encounter any policy or regulatory issues with your use o f AI ? Have you refrained from putting AI based services in production as a result of regulatory	

requirements or due to legal uncertainty?	
Q38: In your opinion, what are the most promising areas for AI applications in the financial sector in the medium term and what are the main benefits that these AI-applications can bring in the financial sector to consumers and firms?	Fairer Credit decisioning: Automated underwriting Predictive modeling: Fraud detection and reduced false positives Default prediction for better credit decisioning and underwriting AML compliance & investigation of false positives Natural Language Processing Answers to complex question in plain language Trend analysis from news feeds, filings, research etc., in assessing impact and market fluctuations Cyber Security Compromised login credentials (behavioural biometrics) / security breaches Account reconciliation automation Consumer advice and self-service (chatbots); Personal finance management; conversational banking Switching services, subscription management and automated bill pay
Q39: In your opinion, what are the main challenges or risks that the increased use of AI based models is likely to raise for the financial industry, for customers/investors, for businesses and for the supervisory authorities? Please specify what other main challenge(s) or risk(s) the increased	Rating system – need to check consultation paper **Financial Industry** 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) 1.1. Lack of legal clarity on certain horizontal EU rules 1.2. Lack of legal clarity on certain sector-specific EU rules

use of AI-based models is likely to raise for the financial industry:	1.3. Lack of skills to develop such models 1.4. Lack of understanding from and oversight by the supervisory authorities 1.5. Concentration risks 1.6. Other **Consumers/Investors** 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) 2.1. Lack of awareness on the use of an algorithm 2.2. Lack of transparency on how the outcome has been produced 2.3. Lack of understanding on how the outcome has been produced 2.4. Difficult to challenge a specific outcome 2.5. Biases and/or exploitative profiling 2.6. Financial exclusion 2.7. Algorithm-based behavioural manipulation (e.g. collusion and other coordinated firm behaviour) 2.8. Loss of privacy 2.9. Other **Supervisory authorities** 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant)

	3.1. Lack of expertise in understanding more complex AI-based models used by the supervised entities 3.2. Lack of clarity in explainability requirements, which may lead to reject these models 3.3. Lack of adequate coordination with other authorities (e.g. data protection) 3.4. Biases 3.5. Other
Q40: In your opinion, what are the best ways to address these new issues? Please specify what other way(s) could be best to address these new issues:	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant) 3 (neutral) 4 (rather relevant) 5 (fully relevant) New EU rules on AI at horizontal level New EU rules on AI for the financial sector Guidance at EU level for the financial sector Experimentation on specific AI applications under the control of competent authorities Certification of AI systems Auditing of AI systems Registration with and access to AI systems for relevant supervisory authorities Other
Q41: In your opinion, what are the main barriers for new	Rating system – need to check consultation paper 1 (irrelevant) 2 (rather not relevant)

RegTech solutions to scale up in the Single Market?	3 (neutral) 4 (rather relevant) 5 (fully relevant) **Providers of RegTech Solutions:** Lack of harmonisation of EU rules Lack of clarity regarding the interpretation of regulatory requirements (e.g. reporting) Lack of standards Lack of real time access to data from regulated institutions Lack of interactions between RegTech firms, regulated financial institutions and authorities Lack of supervisory one stop shop for RegTech within the EU Frequent changes in the applicable rules Other **Financial Service Providers:** Lack of harmonisation of EU rules Lack of trust in newly developed solutions Lack of harmonised approach to RegTech within the EU Other
Q42: In your opinion, are initiatives needed at EU level to support the deployment of these solutions, ensure convergence among different authorities and enable RegTech to scale	

up in the Single Market?	
Q42.1: Please explain your answer to question 42 and, if necessary, please explain your reasoning and provide examples:	
Q43: In your opinion, which parts of financial services legislation would benefit the most from being translated into machine-executable form? Please specify what are the potential benefits and risks associated with machine-executable financial services legislation:	
Q44: The Commission is working on standardising concept definitions and reporting obligations across the whole EU financial services legislation. Do you see additional initiatives that it should take to support a move towards a fully digitalised supervisory approach in the area of financial services?	

Please explain your reasoning and provide examples if needed:	
Q45: What are the potential benefits and drawbacks of a stronger use of supervisory data combined with other publicly available data (e.g. social media data) for effective supervision? media data) for effective supervision? Should the Please explain your reasoning and provide examples if needed:	
Q46: How could the financial sector in the EU contribute to funding the digital transition in the EU? Are there any specific barriers preventing the sector from providing such funding? Are there specific measures that should then be taken at EU level in this respect?	
Q47: Are there specific measures needed at EU level to ensure that the digital transformation of the European financial sector is environmentally sustainable?	

Additional Information	
Summary:	