European Payment Institutions Federation aisbl

15 JUNE 2017

EPIF RESPONSE TO COMMISSION CONSULTATION ON FINTECH

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised Payment Institutions (PIs) and other non-bank payment providers as our members offering services in every part of Europe. EPIF thus represents roughly one third of all authorized Payment Institutions in Europe. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- Acquirers
- Money Transfer Operators
- FX Payment Providers
- Mobile Payments
- Payment Processing Service Providers
- Card Issuers
- Third Party Providers
- Digital Wallets

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as providers for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

GENERAL COMMENTS

Financial technology has the potential to democratise financial services across the EU. Consumers expect to be able to shop online, transfer money, and purchase financial services products online and cross-border as quickly and as easily as sending an email or a text message. With the right technical and regulatory pan-European framework, financial technology companies can provide consumers with the flexible, convenient and safe level of service that they now expect from any other industry.

The Commission's goal of achieving a truly Digital Single Market is accelerated by these developments. Faster, cheaper and more convenient payments networks across the EU, as well as a mostly harmonised regulatory landscape converge to make Europe one of the most integrated marketplaces in the world- and financial technology companies play a crucial role in supporting this. From easy cross-border payments, to hastening the advent of online identity verification, FinTech is making it easier for European citizens to shop, and compare services cross border. As such, regulation must help support financial technology firms to operate in multiple European jurisdictions. Ensuring harmonisation throughout Member States, as well as a review of contradictory legislation, will allow FinTechs to seamlessly offer products and services cross border, as well as facilitate pan European commerce. Indeed, if FinTechs and incumbents are enabled to offer their services cross-border, the consumer will benefit from and injection of competition into a long stagnant market.

The regulatory framework in the EU helps enable and drive these developments - but more can be done. Online identity regulation is inconsistent (consider the opposing stances of eIDAS against the 4th Anti-Money Laundering Directive), and recent developments have arguably seen the balance between user convenience and security disproportionately shift towards cumbersome security checks. The three principles that have been proposed to guide the regulatory approach to FinTech, of tech neutrality, proportionality and integrity, should help EU FinTech thrive. Most EU FinTechs are, of course, fully regulated under pre-existing legislation, such as the E-Money Directive or PSD (I and II). Any additional legislation considered or produced by the Commission must also be future proof, harmonised and risk based - with the opportunity to review regularly as new markets and technologies emerge.

RESPONSES

1. Access to FS for consumers and businesses

1.1. What FinTech applications do you use and why? What areas would you like to see more processes?

- Whilst recognising that this question is aimed at users rather than practioners, it is worth mentioning that the term "FinTech application" includes all forms of financial technology, many of them would not automatically come to mind with the terminology used. Every app, every website, every IVR system, every automated back office process, is "FinTech".
- Many businesses and startups already use FinTech solutions internally for different aspects of their businesses. While this is dependent upon the needs of the company (anything from ID verification to money transfer has been disrupted), each service is typically embraced as a result of similar factors.
- FinTech is merely the application of technology to financial services - and no financial services company can afford to miss the opportunities that technology provides.
- Moreover, financial technology companies are gradually making small progress towards providing infrastructure for banks themselves, as well as directly to consumers. This evolution is years away from becoming a defined shift- but the cost and convenience for providers are big draws in certain verticals for incumbents to embrace new FinTech solutions.

Whilst European legislation relating to payments has led to a plethora of companies emerging from the continent such as Kantox, Adyen, TransferWise, Trustly, there are still not as many established FinTechs in the non-payments space. In particular, EPIF would like to see greater support for cross-sectoral financial services FinTechs, particularly in the KYC, AML and fraud arena.

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

Whilst EPIF members do not provide regulated financial advice, technology improves the ability of businesses to offer execution-only services to consumers who do not require advice. It also, clearly, reduces the cost to serve, both in terms of providing fully automated or semi-automated advice, opening up investment products to a wider group of potential customers.

We would emphasise that automated advice should not mean a reduced focus on giving good advice. Far from it. Compliance needs to be able to cope with new delivery channels so as to continue to protect consumers.

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

- Reliability: Increased use of robo-advice, particularly with regard to retail investment, can often be more reliable than an individual portfolio manager, as the algorithms involved can be seen to eliminate human error in this particular field (as well as spare the investor the considerable expense of active management fees).
- The benefits of automated portfolio management has been noted by incumbents not just FinTechs.
- AI for fraud detection can mimic the steps taken by a human analyst- with a lower cost scalability. New AI fraud detection can simultaneously look at the data points provided, and scan IDs (searching for the same anomalys as an individual), but also has access to multiple other data points, such as IP latency (to measure the distance from the IP to the address given by the user) and keystroke analysis. The hope is that with increased cross-industry adoption, the fraud prevention AI service may be able to predict fraudulent patterns before they occur- if the data pool is wide enough.
- Moreover, robo-advice provides an opportunity for greater oversight and consistency which is not available to supervisory agencies when scrutinising human advice. Human advice is subjective, and each decision is reliant on individuals following guidelines- which is harder to record.
- Nevertheless a reasonable level of scrutiny should be considered that is not burdensome to businesses, consistent with a risk based approach.

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

No comment.

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

- Key risks would be data storage and retention - and therefore compliance with existing legislation
- However, EPIF would recommend that the challenges and risks cannot be considered without also recognising the tremendous opportunity that artificial intelligence provides to reduce costs for consumers and increase consistency of outcomes.
- All measures to be taken should be risk-based with a prior assessment of the possible negative impact on innovative business models.

Crowdfunding

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

No comment.

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

PSD2 has taken an important step towards supporting the roll out of non-bank financing options across Europe. The introduction of AISPs will allow digital comparison tools - as well as financing companies - to offer consumers and SMEs tailored quotes based on their individual requirements. As such, it is integral for further innovation and consumer benefit that the implementation of PSD2 at a Member State level is comprehensive, and ensures that consumers have the right to use software to give Third Party Providers (TPPs) consent to provide products and services based on full direct access to the user's data.

The regulatory infrastructure that underpins consumer and business finance remains fragmented along national lines. Within the framework of the Consumer Credit Directive, Member States have adopted disparate requirements regarding credit licensing, conduct requirements and interpretations of certain alternative lending structures. This has created significant barriers to entry and to scale, and hindered the development of scalable, pan-European FinTech solutions in the credit sector. We would therefore recommend more regulatory harmonisation at EU level in the credit space, by strengthening the role of the Home State supervisor and the passporting principle, which would decrease Member State discretion and contribute to a pan-European framework for FinTech solutions in the non-bank financing space. We therefore welcome the Commission's Consumer Financial Services Action Plan, and specifically the action point to introduce common creditworthiness assessment standards and principles.

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

Transparency in the provision of any financial services product will always be supported by EPIF members. Where consumers can shop around, compare investments and returns, the market will function far better. In the case of these new investment, crowdfunding platforms, the industry should be partly responsible for educating the public. These new products present investment opportunities to a whole new demographic of people, and the associated risks should be clear.

That being said, crowdfunding does not solely apply to businesses. Many of the vendors on these sites are looking to finance a project, like a podcast or exhibitions or their healthcare, that are not offering their investors traditional, monetary returns. In these cases, self regulatory initiatives, provided this information is made clear either by the platform or by vendors, are more than sufficient.

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

Sensor data analytics are particularly useful in the detection of fraud and other financial crimes. However this relies on providers having up to date IT infrastructure and collecting the data that allows providers to make accurate decisions such as IP address, device, time of day, browser, etc.

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

EPIF members do not use big data to discriminate on price as that would mean that providers are using discriminatory price practices based on user behavior. EPIF members have fair, transparent and non-discriminatory pricing structures.

1.11. Can you please provide further examples of other technological applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

Automated money management solutions are becoming increasingly popular. FinTechs like Plum and Moneybox, that automatically calculate and transfer your savings every month based on past patterns, and monthly outgoings, provide consumers short-term solutions for long-term financial health. The low cost introduction of robo-advisors also increases the accessibility of wealth

management to a whole new demographic of people, who couldn't previously afford to retain advice.

As with the digital comparison tools, they depend heavily on the introduction of functional open banking infrastructure, with adequate protections for consumers, and consistent access for TPPs (as long as they remain licensed, compliant and with consumers understanding and consent).

Digital wallets – enabling consumers to load money into their wallet and spend it at retailers – has brought e-commerce to both small businesses and consumers who may not have been adequately served by more traditional providers. Similarly, prepaid products provide access to online services for cash-based consumers or consumers who choose not to use their bank accounts online.

2. Bringing down operational costs and increasing efficiency

2.1. What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

- Many product verticals in retail financial services are provided by FinTechs at a lower cost, and greater convenience to businesses.
- Collaboration within the FinTech community, but also with traditional financial service companies, is relatively commonplace, and many such businesses will look to other disruptors to provide their internal processes. Some members, for example, may turn to digital verification specialists or innovative payment processors to perform their back end functions. Partnerships allow banks to reach more consumers and explore new product offerings and markets. For the FinTech, they ensure that appropriate controls are in place, while providing funding and immediate scale to the service.
- As noted above it is payments that hold the most promising use cases currently, as a result of innovative and technology neutral legislation from the Union.

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

Updating and developing the payments infrastructure across Europe would be directly beneficial for the majority of financial technology companies. With the introduction of SEPA, the European

payments structure has begun to modernise (though it is not without its flaws), and with the upcoming implementation of the SEPA Instant Payments Scheme, it will once again be improved. However, the introduction of the scheme is not enough.

The fact that the SEPA Instant Payment Scheme will be optional, as well as developments of national Instant Payment solutions, might fragment how banks implement the solution, causing further complexity in the market due to different availability and commercial conditions. The EU should ensure the interoperability of these solutions from a technical perspective and in respect of scheme rules, to allow cross-border financial retailers to adopt a single standard across the EU.

The cost of direct membership to SEPA prevents direct participation for PSPs, or smaller challenger banks. In the coming months, the UK government will be piloting a scheme that will allow PSPs and challengers to open direct settlement accounts, and plug directly into the UK's Faster Payments Scheme. The changes will drastically reduce costs for institutions that are currently accessing FPS indirectly, through partners who have been known, anecdotally, to charge PSPs up to two times the cost of the payment. In order to support a world leading FinTech ecosystem, the EU should look to update, and improve access to vital payment infrastructures.

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

As with any disruptive technology in any industry, the EU should predict shifts in the labour market accordingly. While the shifts caused by FinTech are by no means as radical as those triggered by transport companies like Uber given that FinTech is not based on 'shared economy' employment practices, they will markedly change the landscape in financial services. For example, the rise in digital or automated KYC would radically reduce the cost and increase the convenience of some services for consumers, but may also see a small number of jobs in manual KYC to be reduced.

However, FinTechs need a highly skilled digital workforce and by reducing the costs to businesses and consumers they increase their investment and spending power enabling a more rich and diverse economy. Moreover, with the market creating potential of technology there will be new firms and new jobs emerging. Such as from the introduction of AISPs and PISPs in payments, as with firms such as TransferWise or Kandox that have emerged from PSD1.

Regtech: reducing compliance costs

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

The cost of compliance is particularly high for non-banks which have the opportunity to passport cross-border, and many potentially innovative, low cost ways to ensure a business's compliance are often overlooked. The developments surrounding digital identity verification are one of the most promising uses of RegTech in recent years. Online verification procedures and KYC is far more convenient for users without compromising security. A harmonised EU wide online (i.e. non-face-to-face) KYC framework would facilitate the introduction of a truly cross-border financial services market, and markedly reduce the cost of compliance for digital businesses.

Moreover, the lack of harmonisation at an EU level is a challenge to the implementation of online verification. The 4th Anti-Money Laundering Directive (AMLD) and the eIDAS regulation take seemingly opposing stances to online verification. The 4th AMLD still takes the approach that online verification is high risk, and goes some way to discourage businesses from doing so. eIDAS on the other hand, encourages the opportunities that go along with providers being able to establish relationships without physical verification.

Therefore, a wider acceptance of remote and seamless identification methods in the Member States is needed. In order to comply with AML requirements without disrupting the consumer experience, new methods of identification and verification methods should be promoted. Obtaining approval for a remote identification method in 28 Member States, if at all, is costly and time-consuming. eIDAS intended to do so, but failed due to the limited scope. It only promotes methods that are not widespread among consumers.

While there are important privacy and security issues to consider, a centralised, pan-EU eID infrastructure would allow FinTech and RegTech companies to conduct convenient, low-cost and effective KYC and due diligence checks, enabling them to scale across the EU.

2.5.1. What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services?

Cloud computing infrastructure is yet to be adopted by many incumbents. There is still sparse regulatory guidance for the use of cloud computing by financial services firms, and is being primarily adopted in the 'low risk' areas of customer data due to the sensitivity of the information held by some financial services firms. Liability issues need to be clarified. It should perhaps also be noted that there are extensive audit requirements placed on outsourced cloud computing, which can cause issues when a Service Level Agreement is deficient, or does not cover the Right to Audit. Cloud providers may be reluctant to allow a fully comprehensive audit.

The relationship between TPPs and their clients are more complex than typical IT outsourcing relationships. Clients, the financial services firms, must be assured that the provider is industry

compliant, and integratable with their in house IT systems- without being unduly locked into one provider, and unable to shop around.

Cloud computing regulation is out of step with the needs of consumers. For instance, under current regulations most Member States require providers to store customer data locally, even if a consumer is located in another country on the other side of the world. The implications for a European consumer based in Japan or Australia of this is slower speeds, unacceptable to modern consumers. Moreover, it is unrealistic to require providers to own their data storage when this service is so much better provided, and much more cheaply, with an outsourced provider. Differing approaches to privacy regulation globally present challenges to any user of cloud computing services provided by primarily US companies. Further collaboration between European, US and Asian regulators would be welcome, as would similar global collaboration on cyber-security.

The use of cloud computing in big data analytics is burdensome for providers. The process the data must move through, the anonymisation of personal data in the bank's private cloud, to be transferred to the public cloud for processing and then transference back to the bank's internal cloud for re-identification to analyse and propose the necessary products for consumers.

For incumbents, there are also legacy IT systems that are barriers to uptake of cloud computing solutions.

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

Yes, although we would of course encourage more competition to reduce costs and increase quality more rapidly. There should be steps taken to ensure that clients are able to easily switch provider. Solutions must be integratable with their in-house IT systems, yet clients must be able to change providers with minimal difficulty to ensure real competition in the market.

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

We would expect, given the commercial pressure from clients, that cloud solution providers will continue to reduce costs and increase quality of data storage. Moreover, SLA's should be required to include a Right to Audit, to ensure that cloud providers are compliant with the extensive regulation placed on financial services firms.

Distributed Ledger Technology

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

No comment.

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

Blockchain technology, and crypto-technologies, are, in some cases, very much in their infancy. The lack of a common platform or unified approach to their development is holding back the maturity of these technologies. With proportionate intervention and guidance from a government, projects like cryptocurrency, could overcome their potential security issues, and the risks could be mitigated.

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

As stated above, the lack of regulatory guidance, or government intervention, has held back the maturity, usability and safety of cryptocurrencies. The EBF has recommended that services at the interface between traditional and virtual currencies become obliged entities under the Money Laundering Directives, and EPIF would agree.

Outsourcing and other solutions to boost efficiency

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

At entry level there is some confusion with regard to what constitutes outsourcing. Outsourcing can be a very efficient way of reducing costs to providers. We would therefore welcome further guidance that encourages and supports outsourcing. Today, firms no longer outsource end-to-end activities, but rather use piecemeal technology solutions to create larger solutions. Some of those solutions are retained in-house while others are outsourced to third parties. This is especially true when considering RegTech solutions. The regulatory framework should be updated in light of this new reality to provide companies with more flexibility in how they manage the risks associated with using external service providers.

Thus far, certain Member States have cumbersome outsourcing requirements. For instance, under PSD1, some member states (e.g. Spain) required prior supervisory authorisation for the outsourcing of essential functions. The transposition of the PSD2 is still ongoing and such inconsistencies should be avoided.

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

As stated above, more could be done to ensure the appropriate guidance is given to support reasonable outsourcing as a way of reducing overheads for high-growth start ups.

Other technologies that may increase efficiency for the industry

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

No comment.

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

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

Specifically the Payment Services Directives and Electronic Money Directives are good pieces of legislation but there are still examples where legislation specifies specific technologies or practices which, whilst at the time of drafting are up-to-date, by the time of implementation are not the most efficient or appropriate for the best consumer outcomes given the development on the ecosystem.

Specific examples would be:

- Strong Customer Authentication provisions which were too specific in the original legislation meaning that at the time of implementation regulators do not have the flexibility to provide the best consumer outcomes. The approach taken by the Commission and EBA favours banks and traditional payment methods over innovative FinTech solutions that aim to improve the consumer and merchant's experience. The rules do not taken into account the complex payments value chain that results from the introduction of new FinTech solutions, notably through the first Payment Services Directive. This will result in a confusing and

complex experience for consumers, who may be faced by multiple SCA challenges from multiple PSPs for the same payment transaction. It will furthermore hinder the development of FinTechs who will see little incentive to enter the payments market.

- The EBA's approach to disallow direct access to the consumer-facing online interfaces of the ASPSP in the Regulatory Technical Standards under PSD2.
- The surcharging provisions in PSD2, which, while thoroughly laudable in their intention did not foresee payments FinTechs that offer cards as their most expensive pay-in methods with the net effect that consumers are going to pay more for other, far cheaper, payment instruments to subsidise card users.
- Recent AML legislation contradicts innovative solutions in the FinTech sector without providing added value in terms of fighting ML/TF. This is especially true with regards to the prepaid sector and the online use of prepaid cards which disregards the extensive possibilities to monitor financial transactions and mitigate the risk of the products being abused.
- As stated above, an EU-wide harmonized approach regarding the approval of seamless remote identification methods is needed. Instead of considering remote identification and verification as high risk (AML legislation), innovative online methods provide at least the same level of security and even more convenience than offline verification methods.
- As already noted, FinTech companies need consistent, open and fair access to bank accounts in order to carry out their activities. Whilst we welcome the provisions of the revised Payment Services Directive, we remain concerned that national implementations may not result in the easier access the Directive is intended to provide. The regulatory infrastructure that underpins consumer and business finance remains fragmented along national lines. Within the framework of the Consumer Credit Directive, Member States have adopted disparate requirements regarding credit licencing, conduct requirements and interpretations of certain alternative lending structures. This has created significant barriers to entry and to scale, and hindered the development of scalable, pan-European FinTech solutions in the credit sector. We would therefore recommend more regulatory harmonisation at EU level in the credit space, by strengthening the role of the Home state supervisor and the passporting principle, which would decrease member state discretion and contribute to a pan-European framework for FinTech solutions in the non-bank financing space. We therefore welcome the Commission's Consumer Financial Services Action Plan, and specifically the action point to introduce common creditworthiness assessment standards and principles.

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

FinTech innovation and uptake is impacted by a number of things: access to capital, trust from consumers, and regulatory support for innovation.

The Commission should also consider taking more action against discrimination on grounds of residence in the European market in retail financial services and, if necessary, to complement the planned general proposals to end unjustified geo-blocking, with further legislative initiatives targeted specifically at the financial sector. In doing so, they could maximise the uptake of FinTech solutions throughout the EU, and work towards a truly digital single market.

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

Yes, but greater cross-border collaboration such as that in PSD2 for other financial services verticals will drive innovation.

The lack of regulatory harmonisation in a number of policy areas (e.g. AML, credit, consumer protection, cybersecurity, data protection) remains a significant barrier for FinTechs to scale across the EU. EPIF would recommend more regulatory harmonisation at EU level, by strengthening the role of the Home State supervisor and the passporting principle. This would decrease member state discretion and contribute to a pan-EU regulatory and supervisory framework.

Financial services policymakers and regulators should begin to think like FinTech policymakers and regulators. FinTech is not a single undertaking, but rather represents technology shifting a broad range of traditional financial services offerings. Regulation must treat each of those services individually, identify the particular risks associated with that service, and create regulation that is based on the service rather than the entity providing the service.

EPIF encourages regulators to foster growth and innovation by cooperating with innovators and by exploring sandboxes. This mechanism eases regulatory compliance without jeopardizing consumer protection and creates safe spaces for product testing. The experiences in the UK and around the world show that, at a minimum, sandboxes have fostered cooperation between innovators and regulators to embrace necessary norms and user protections as part of their design terms. This can only serve to promote a better ecosystem, whatever the tangible outcome of the pilot projects in these sandboxes.

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

The lack of an EU wide sandboxing regime means that many start-ups are unable to start to offer their product across the EU. As a result, they may struggle to understand if they have a market for their innovation in other member states. Indeed, because businesses may struggle to see if their product is viable cross-border they may be disinclined in the early stages, after transitioning out of the sandbox, to try and navigate the different regulatory demands of each member state- without first demonstrating their is an appetite for their product in that state.

Moreover, while the levels of flexibility given to each individual Member State in fighting financial crime is necessary for each country to assess individually the threat posed to their financial stability, the ability for Member States to increase their demands on businesses, often disproportionately, can also be seen as a barrier for FinTechs to trade cross-border. For example, the introduction of Central Contact Points which may be introduced at the discretion of each member state will be burdensome to small businesses. Each Contact Point would require an estimated €100,000 to run, per year.[1] Moreover, consumer protections in each Member State vary hugely. The cost for a start-up to comply with each member states requirements is a huge, costly endeavor. As such, we would encourage a unified set of standards.

Also, many leading FinTechs may choose to scale up with investment from third countries such as the US, instead of in Europe. For instance, it is more profitable for firms to initially float their IPO on the US stock market. Also, the US marketplace makes it easier for investors to recoup their profits, and FinTechs to unlock more capital - without forcing founders to go public or dilute their stake in the business. Recapitalisation frameworks in the US make it easier for owners to retain control of their business, without further diluting their interest by bringing on more investors.

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

[1] Research conducted by the Electronic Money Association

On the whole there is no need for new licensing categories as all of the current FinTechs should be accommodated within the existing traditional groupings. The vast majority of FinTech applications are already regulated under existing financial regulations. For instance, in the EU, FinTech payment providers have been brought under the regulatory umbrella of instruments like the Payment Services Directive (PSD2), the e-Money Directive (EMD) and the Anti-Money Laundering Directive. Moreover, because FinTech is often driven by enhancing the user experience, non-financial consumer protection regulation also applies to FinTech entities, such as existing consumer protection, data protection and information security rules. However, it may be useful for some cases to update regulatory frameworks to take into account new iterations of traditional business such as crowdfunding platforms.

Rather, it is the regulatory and supervisory approach to financial services that needs to be adapted. In the future, financial service regulators and supervisors are likely to regulate a wide range of companies, not all traditional financial services entities. To remain agile, it is important that supervisors and regulators take a principles-based, industry-inclusive approach that looks at the service provided rather than the entity providing it.

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

It would be useful to build in earlier review periods of existing legislation specifically designed to consult/accommodate new entrants/iterations that had not been considered when the original legislation was designed.

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

The free flow of data is essential for a cross-border offering of financial services. Business is becoming more global every day. Technology, in particular mobile, enables businesses to connect with customers all over the world. Connecting the world through globalisation has helped to democratise financial services and empower small businesses and consumers around the world.

It would be useful to have greater harmonisation to make it easier to share data across jurisdictions within companies so that companies are better able to deliver the single market.

With the tightening of borders around the world, including within Europe, we must guard against the danger of data localisation. Data localisation requirements have a serious risk of unintentional negative economic impact by making it more expensive for companies to operate, disrupting trade

flows, harming job creation and discouraging innovation. We therefore welcome the Commission's upcoming regulatory initiative on this topic. In financial services, restrictions on the free flow of data can have many sources, including local banking secrecy/client confidentiality obligations, in addition to general data protection requirements.

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

Yes, however we would also add awareness of high growth and market creating technologies to enable unforeseen technologies and services to be accommodated where possible in existing regulation more rapidly.

EPIF would also add:

- **The risk-based approach**: whether in payment security, AML rules or elsewhere, we would urge regulators to take an approach that is based on the actual risks of the service, rather than mandating one-size-fits-all blanket rules that are not adapted to the subtleties of each business model and innovative technology.
- **Future-proof**: the EU regulatory approach should be fit for both today's innovations, as well as those of tomorrow. Only an outcomes-based approach can achieve that, where the regulatory framework sets out principles and leaves the method with which to achieve them to innovators in the market.
- **Harmonisation across the EU**: in order to bring the real benefits of FinTech to consumers and SMEs, breaking down national barriers in legislation is critical.

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

Proportionality is key when looking to regulate new start-ups. Established FinTechs are already adherent to the same regulation as incumbents, where they provide the same services. The cost of compliance for new start ups is high, as in many cases, much of the regulation they must comply with seems to have been written with incumbents in mind.

As we have stated above, technology neutrality is vital for delivering enhanced consumer outcomes.

Integrity of the market should be prioritised, alongside the other principles. FinTech can help bring fresh competition and transparency to stagnant markets - which can only drive down prices and benefit consumers. The issues of misspelling and cyber security are by no means unique to any player in financial services - new or otherwise - yet the Commission is right to ensure all possible consumer protections are proportionately applied in line with the services offered by financial technology firms. It is unlikely that the banks will be usurped in providing the base infrastructure to

the financial system, thus the systemic risks mentioned would be in-line with traditional that posed by traditional providers. Moreover, the Bank of England believes that the introduction of new entrants (when supervised correctly) can actually reduce systematic risk.

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

As noted above, the EU as a whole would benefit from a harmonised sandboxing regime through EU guidelines that harmonise various national initiatives. Start-ups would benefit from the ability to understand if they have a market for their innovation in other Member States. Currently, businesses struggle to see if their product is viable cross-border they may be disinclined in the early stages, after transitioning out of the sandbox, to try and navigate the different regulatory demands of each member state- without first demonstrating there is an appetite for their product in that state.

We would also add:

- **Developing EU guidelines on the regulatory and supervisory approach to FinTech supervision**. Financial service regulators and supervisors in the future are likely to regulate a wide range of companies, not all traditional financial services entities. EU guidelines will be essential to ensure a common approach to FinTech supervision that is principles-based and industry-inclusive.
- **Creating interoperability between issue-specific regulators, as well as across borders**: regulators and policymakers should think beyond their specific mandates and national borders. An example of a successful model comes from Singapore, where the Monetary Authority of Singapore has established a FinTech office designed to foster partnership among a variety of government agencies that might impact FinTech.
- **Fostering entrepreneurship**: FinTech companies are just like any other nascent company; they need a friendly business environment in which to start their business and scale-up. This includes simplified and affordable processes to set up a company in a given Member State, as well as access to the right advice, tools and skills.

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

Yes, there are tremendous advantages to pooling expertise as ESAs can learn from other ESAs' experiences speeding up their development.

3.9. Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns?

Yes, as long as the costs are proportionate for the gains and that any Innovation Academy is able to actually drive rapid regulatory development.

3.10.1. Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS?

As stated above, an EU wide regulatory sandbox would be beneficial to start-ups to allow them to test the viability and appetite for their products in different jurisdictions. Thus, when they transition out of the sandbox, there is an incentive to have produced a product that will be able to provide cross border the same financial services product. FinTechs would be less inclined to localise their services for the first few years, as an appetite had been established.

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

Absolutely. This is because operating cross-border can be very difficult for FinTechs who typically do not have access to the same breadth of expertise and experience that incumbents have.

3.11. What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above?

As noted above, expertise and experience is a huge barrier for new entrants. Anything the Commission can do to help with these will be vital to continue a healthy FinTech sector, for example:

- More digestible regulation, for example showing regulations and Regulatory Technical Standards as the EU intends firms to implement them.
- Greater outreach to upcoming firms from regular landscaping of the FinTech ecosystem.
- Ensure harmonization and urge member states not to hinder innovation by implementing contradictory legislation.

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

No.

As mentioned above, Strong Customer Authentication provisions are too specific in the original legislation meaning that at the time of implementation regulators do not have the flexibility to provide the best consumer outcomes, but are tied to the initial primary legislation.

3.12.2. Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

No opinion.

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

No opinion.

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

Open data and source solutions have the potential to allow the tech sector to flourish. Access to open source solutions would accelerate the development of new businesses as well as tech innovations. The European Space Software Repository has already piloted the scheme. Copyright and ownership concerns should be taken into account, especially when the software has not been produced as part of a member state or EU government project.

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

The impact of FinTech on the safety of incumbents is minimal. Even with the introduction of Open APIs, FinTechs, especially in the payments space, are as compliant to the same regulations as the incumbents and assume the same liability for any data breaches.

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

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

The free flow of data across the EU is essential provided that customers are as aware of it as firms can reasonably make them, and freely provide their consent.

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

DLT solutions are simply highly effective means of archiving and storing data. The challenge is to ensure that DLT, like any other archiving or data storage solution, is as secure as it can be reasonably expected to be.

It is essential that the EU and Member States recognise that traditional single site storage is unreasonable for many cross-border firms without compromising consumer speeds. However, it would be useful for the EU to explore the risks and opportunities of future data storage developments particularly with regard to how to ensure there is sufficient competition and ultimately high security and consumer speeds.

DLT should fulfil this but the applications are not yet sufficiently developed for financial information storage and sharing. Using DLT could increase the security of that data, increase speeds for consumers and reduce costs for businesses and consumers.

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

Yes

While there are many pioneering schemes around Europe in terms of digital identity, and the eIDAS regulations brought about new opportunities for providers, a centralised digital identity database in each member state or more excitingly across the EU, like that used in India or Estonia, would allow financial services companies the flexibility to conduct convenient, low cost KYC/CDD checks. The changes would save the consumer time and money while enabling FS firms to sell products cross border. Using DLT could increase the security of that data, increase speeds for consumers and reduce costs for businesses and consumers.

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

The main challenge is compliance with traditional single site storage regulations.

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

No opinion.

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

In the UK, incumbents who receive and reject SMEs looking for financing are by law mandated to pass on the information to specific comparison providers, who may unlock alternative capital raising methods/ or credit for SMEs. It is yet to be seen whether this is an effective measure for increasing information sharing.

AISPs under PSD2 provides the greatest opportunity for increased customer centric information sharing but likewise, it needs to work for consumers.

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

- The regulations in this space already exceed those required by other businesses. Currently, financial service providers are obliged to enforce several layers of requirements, creating a fragmented patchwork of obligations. These include the NIS Directive, the eIDAS Directive, and the General Data Protection Regulation, which all focus in one way or another on securing data and infrastructures. There are also sectorial obligations such as the upcoming PSD2 and ePrivacy Regulation. This is further supplemented by other layers, in particular by the EBA and ENISA at EU level, but also by industry standards such as PCI or ISO27X, which are in effect mandatory under specific contractual obligations with key stakeholders of the financial market, such as the credit cards schemes. As such, we do not see the need for additional cybersecurity requirements for financial service providers.
- Rather, financial institutions need clarity, and ways to reduce the compliance costs by finding ways to eliminate double obligations and related audit constraints. In this sense, EPIF members would welcome the harmonisation of the format and procedures for security incident reporting, which remain fragmented across different EU legislation (e.g. NIS Directive, PSD2, GDPR, Single Supervisory Mechanism). This overlap created redundancies in reporting to multiple competent authorities, as well as utilises resources, which could be better deployed to manage the incident.
- It would also be more beneficial to see the same rules imposed on non-financials that handle PII than more regulation (that is normally outdated before it is in effect) for financial companies.

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

In the case where criminals attack originate from countries with limited cooperation with the EU, it is difficult to track or share information regarding their activities in that jurisdiction. Public/private

partnerships, where possible, would remedy this. The Joint Cybercrime Task Force goes some way to remedy this and coordinate international investigations by drawing on a pool of member intelligence. Security and privacy should be balanced against the need for law enforcement and private sector to draw an accurate picture of criminal activities.

- There are several areas where information-sharing could be improved:
    - Amongst Member States, to ensure that information that is shared by regulated entities with their Home State regulator is properly shared with other relevant member states. A data-sharing scheme between FIUs would be helpful in this regard.
    - Between the industry and law enforcement, by reinforcing channels of communication. A legal framework for data sharing across the public and private sectors for resilience and risk mitigation purposes would be welcomed to ensure more streamlined information sharing, as well as legal certainty for the firms sharing the data, which may be subject to rules that prevent their sharing (e.g. data protection). Such a framework should allow the sharing of sensitive information related to fraud and cyber-attacks at national and cross-border levels.
    - Amongst the industry, but this has been hindered by banking secrecy and data protection regulations that prohibit companies from sharing information with third parties.
    - EPIF therefore welcomes the Commission's review of the framework on combatting fraud and counterfeiting of non-cash means of payment, which also seeks to improve the sharing of information in this field.

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

No opinion.

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

It is actually more simple than new technologies. What is needed is some industry standardisation. It would be useful to implement a more simple information-sharing framework based on key data which should be known about a payer (name, address, account number/IBAN), additional optional data points and what is not reasonable to collect (recipient something). But most importantly there should be a specified format for all of these options and reasonable amount of time to expect a response and to request responses in batches not as they arise.

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

Yes.

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

Digital KYC is not being embraced by regulators. Online KYC would reduce costs and increase convenience for consumers, and technologies such as VideoIdent should be encouraged, rather than blocked, by the EU. As highlighted in question 2.4, the lack of a harmonised regulatory approach is detrimental to the development of online verification, detrimental to the creation of a digital single market in financial services and a barrier to access for consumers.

Information sharing channels with regard to money laundering and fraud are poor. In the private sector, there is reluctance, partially due to a lack of clarity in data sharing regulations, to share information about either trend in suspicious customer behavior, or flag a particular individual as potentially taking part in criminal activities. Information sharing between public and private companies should be reconsidered. In certain jurisdictions, companies may receive requests for information by law enforcement, without ever receiving clarity on whether the particular behavior that sparked the inquiry was indeed indicative of criminal activity.

Additional information from law enforcement can only further empower private companies to identify criminal or suspicious behavior, thus regulatory requirements that prevent constructive information sharing between public and private institutions looked at carefully. Data protection concerns must be respected, though we would encourage the Commission to look into new ways to help private companies identify and fight criminal activity.