Financial Services Consumer Panel
AN INDEPENDENT VOICE FOR CONSUMERS OF FINANCIAL SERVICES

Telephone: 020 7066 9346
Email: enquiries@fs-cp.org.uk

15 June 2017

Dear Sir/Madam

This is the Financial Services Consumer Panel's response to the European Commission consultation on FinTech.

The response is to be submitted via an online questionnaire.

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

In the UK, financial technology (FinTech) firms are increasing in number and some of these firms are harnessing big data and analytics. For example, we have witnessed a rise in the number of 'robo-advisers' and online platforms over the past 2-3 years and consumers are beginning to invest more money through this route.

FinTech firms are challenging traditional financial business models and are likely to play a key role in firms moving towards less capital-intensive business models, where (after the initial investment) firms benefit from economies of scale with lower ongoing costs. However, it remains to be seen whether those lower costs and increased competition will translate into lower costs and better services for consumers.

The Panel also believes that more clarity around the regulatory framework governing FinTech solutions and ensuring that regulators are able to effectively supervise emerging practices will be key to ensure FinTech delivers tangible benefits to consumers.

1.2 Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance etc.) and at what pace? Are these services better adapted to user needs? Please explain.

Online investment platforms and services in the UK have evolved dramatically over the last decade. The combined forces of technology and regulation have changed the landscape beyond recognition. The UK's first 'robo adviser' was launched to a flurry of industry interest in 2012 and many more have emerged since[1].

[1] Boring Money Ltd. 'Assessing online investment and advice services': https://www.fs-cp.org.uk/sites/default/files/final_online_investment_and_advice_services_summary_report_bm_30_regulator_doc_05_12_2016.pdf

A recent Panel position paper indicates that, despite rules already being in place to protect consumers in this sector, there are serious shortcomings that can lead to poor consumer outcomes. Poor practice relating to transparency, clarity and consistency mean some firms are not treating their customers fairly and are failing to meet their needs. Please see our response to 1.8 for more detail.

In fact, many consumers are not getting regulated advice at all, but an online journey that looks like advice but ends in the consumer buying a product 'execution only', which means their protection is much reduced. Panel research shows that consumers do not understand the difference between advice and guidance, and whether they are protected or not.

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

Yes.

In an increasingly digital world, algorithms are being used to make decisions in a growing range of markets. This affects retail consumers in a number of financial services markets, including credit, insurance, and 'robo' advice. Effective oversight and supervision will be crucial to avoid widespread consumer detriment.

For example, it is unclear how firms will be able to explain to consumers the decisions that have been made using complicated algorithms and machine learning. Supervisory oversight is therefore crucial. The Panel would argue that firms that have algorithms at the heart of their business models should set-up ethics committees to discuss and explain decision-making driven by algorithms. These ethics committees should also have a requirement to inform the supervisory authority immediately as they become aware of any unusual findings from management information on the algorithms. The EU should set the criteria for the minimum MI that is reviewed by ethics committees.

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)?

Service providers using algorithms should ensure that the requirements and suitability reports they use are as comprehensive as the fact finds used by non-algorithmic providers. Service users should not be worse off because the products or services they opt for are driven by algorithms.

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?

The Panel has recognised a number of challenges and risks brought about by the increased use of data analytics, some of those include:

- Establish workable and fair social norms for the collection, storage, acquiring and usage of consumer data.
- Understand layers of data and how the consumer can own and control different types of data.

- Prevent discrimination in accessing products and services resulting from consumers' choice not to share their data with service providers.
- Account for algorithmic decision making in a world where algorithms now drive decision-making in ways that touch our economic, social and civic lives. In order for this not to lead to consumer detriment, there will need to be a framework in place which allows for transparency throughout the decision-making process. Opening algorithms to regulatory scrutiny could enable relevant stakeholders to monitor, audit and criticise how those systems are functioning.
- Keep-up with the speed of innovation. Regulators need to have sufficient resources and capability to keep up with developments in this sector.

In light of the above, we would invite the EC to consider the following:

- Design a neutral, not for profit, infrastructure that enables people to store their data in a safe place and consent to share it with others in a controlled way
- Work to enable traceability of data
- Learn from the health sector and set up an ethics committee to assess and advise on the ethical implications of big data and changes in the financial services market
- Incorporate ethics into the governance structure and decision making of firms using big data, overseen by an ethics committee (reporting to the company's board), which is held to account by a separate independent user-focussed Panel (funded by the firm) which has recourse to the regulator if it is not satisfied with the decisions taken to guard privacy and freedom.
- Undertake further research on the impact of big data on the provision of products and services and publish an annual report monitoring developments including reference to negative unintended consequences and how these will be mitigated.
- Invest in 'regtech' and the ability to supervise and enforce against GDPR and other relevant regulations effectively and promptly.

The Panel would also call for specific guidance on how the principles introduced by the General Data Protection Regulation (GDPR) should be implemented in retail finance.

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

There is currently no pan-EU regulatory regime for crowdfunding, which has held back the development of the sector. A specific crowdfunding regime at the EU-level would ensure investors across the EU are protected equally and enable more crowdfunding platforms to operate cross-border by boosting investor confidence.

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, crowd-funding, invoice and supply chain finance?

The Panel supports the development of investment based crowdfunding and peer to peer platforms as it can give consumers direct access to a wider range of investment options. However, a clear legal framework guaranteeing consumer rights should underpin further developments in this sector.

The current regulatory framework is not designed with new FinTech solutions in mind; this spurs regulatory arbitrage and threatens consumes. As crowd investors are prone to a high risk of capital loss markets, there should be at least effective warning for consumers. The recently review Prospectus Directive which substantially raises the exemption thresholds for equity crowdfunding projects (up to EUR 8 million) makes this even more pressing.

Regulatory and legislative efforts at the EU level should focus primarily on developing a cross-border framework guaranteeing minimal consumer protection.

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?

Self-regulation is not sufficient and the lack of transparency and consistency in online investment platforms could cause wide spread consumer detriment as the market continues to develop further.

In a recent position paper on online investment platforms used by UK retail investors the Panel found that:

- The regulatory distinctions between guidance and advice and its associated implications, such as recourse to the Financial Ombudsman Service (FOS) and Financial Services Compensation Scheme (FSCS), were not clear.
- References to the FOS and FSCS were not prominent on many websites.
- Costs and charges were poorly communicated, often misleading and difficult to find. They were typically disclosed in a way that made it difficult for consumers to understand how much they would be paying and what for. Only one of the 15 consumers who used the websites was able to calculate correctly what the total cost of a £1,000 investment would be.
- Several firms promoted 'all-in' fees that did not include additional costs borne by the consumer, such as underlying fund charges. Additional costs were always provided separately to fees and were always in smaller fonts, at the bottom of pages or hidden in charts.
- Firms did not use language that consumers understood. Whilst some websites were better than others, jargon was prevalent and explanations were frequently misleading. The language used generally assumed an unrealistic level of familiarity even with concepts that might be expected to be widely understood, such as 'funds' and ISAs.
- While the language used in risk profile questionnaires was usually clear and well understood, the language used to describe portfolios was generally unclear and confusing to consumers.

All of the above points to the need of regulatory oversight as the sector continues to develop.

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?

n/a

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

Insurers' increased use of big data to inform risk and pricing strategies is likely to restrict access for certain segments of the population. The use of individualised micro risk assessments means that some people are likely not to be served at all. Other will pay much higher premiums. Conversely, some consumers, for instance

some young drivers or elderly travellers, should pay lower premiums than they do now because their individual risk is lower than that of their peer 'risk group'.

In time, increasingly individualised risk assessment could have a significant impact on risk pooling and individual premiums. A reduction in risk pooling would fundamentally alter the structure of the insurance industry.

The level of transparency in risk profiling is another issue of concern. It is unclear now how firms assess risk and it is impossible for individuals to know if they are getting value for money as a consequence. If firms use algorithms to assess risk, consumers cannot check the methodology, or correct their own behaviour or attributes to improve their 'score'. There is therefore a need to ensure that decisions made based on data analytics can be challenged and remedied appropriately.

The nature of the data being used is also sensitive as firms will often rely on personal data. Any regulatory approach to this application should therefore need to strike the right balance between facilitation and compliance with the GDPR.

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?

Some firms have begun to use consumer transaction data to build transparent credit score-cards, which can help consumers with thin credit files to access credit when they were previously excluded.

Some firms are also using data to help people with new insights about their spending patterns which can significantly help change spending and saving behaviours. Added to this is the possibility of 'round up' saving which 'rounds up' spending on items like coffee to the nearest pound and moves the 'pence' to a savings account, helping people save easily and regularly with minimal effort.

Other AISP services are alerting people to the need for financial advice and enabling them to share their financial profile directly with independent financial advisers, opening up financial advice to those who may not have previously considered it; and at a pertinent moment when someone may be more likely to take action. There is the opportunity to explore doing the same for people whose income may suggest they need help with debt management.

Again, other firms are helping people manage their spending by using technology to block spending over certain limits pre-set by the customer; or blocking spending after a certain point in the evening when people may be more vulnerable to spending spontaneously.

These initiatives improve people's economic resilience. The benefits of seeing small savings pots increase can also psychologically make managing money more engaging.

However, technological applications could create more conflicts of interest, exploit asymmetries of power or exacerbate financial exclusion.

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?

n/a

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?

There is a need for the EU to ensure that liability regimes are appropriate and easy to understand navigate, both for consumers and firms.

See response to question 2.4 on RegTech.

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 a change?

In order to avoid consumer detriment, it will be important to ensure FinTech companies place consumer protection at the heart of their corporate culture and that their staff receive proper training so that consumer protection principles aren't foregone as a result of FinTech solutions.

Additionally, consumers should continue to have access to an employee as a port of call in order to challenge, appeal and resolve issues associated with FinTech solutions.

Regulators also need to keep up with the speed innovation and ensure they have the skills and tools to supervise and regulate FinTechs.

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 the EU level to facilitate their development and implementation?

The FCA recently published a report that summarises industry views on the emerging RegTech sector. [2] In general, it was agreed that RegTech would have a positive impact on the financial services industry and would help to boost competition in the sector. The Panel is supportive of initiatives that support the streamlining of regulatory reporting at both the UK and EU level so long as they are implemented with the consumer interest in mind.

In particular, the development of RegTech should not create new risks for the protection of customers' privacy and personal data. National financial services regulators who are not familiar with these issues should either 'skill-up' or work hand in glove with authorities competent for privacy and personal data protection (i.e. the Information Commissioner in the UK).

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

n/a

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

[2] https://www.fca.org.uk/firms/innovate-innovation-hub/regtech

n/a

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

n/a

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

While DLT based FinTech firms have increased in number over the past 3 years, DLT is not widely used in the UK's financial services industry.[3] DLT could enhance some activities in future however, for example automating simple processes such a recording client data for Know Your Customer and anti-money laundering purposes.

The adoption of DLT could take many forms and firms face a variety of challenges before widespread use and any resulting benefits might materialise. It is reasonable to assume that a number of DLT systems will need to interact and share data between one another and with non-DLT legacy systems. Therefore, at this stage, it may be difficult for DLT to be fully incorporated in the existing core processes. While the volume of successful Proofs of Concept has been an indication of market interest to date, what is still uncertain is the future likely breadth and depth of market adoption. Considerations such as the ease and cost of adoption will be essential.

Until recently, we have not seen much consideration by firms of the regulatory consequences of deploying DLT solutions in regulated financial services. This may be because, up to this point, firms are still developing their own understanding of the technology and realistic cases where it could be used. However, with firms devoting increasing attention to DLT solutions, it is important national and European regulators remain abreast of developments in this area and how it impacts their regulatory approach.

2.8 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?

There is still no firm regulatory framework in place for the potentially disruptive blockchain technology to be used by financial services firms in the UK. The FCA recently published a discussion paper on the potential uses of DLT as a conversation starter and as a result of having exposed to the technology via its 'regulatory sandbox' initiative.

There remain challenges that may not be addressed as DLT is still at an early stage. Those involved in designing DLT products must bear in mind existing rules and the fact that using DLT technology does not exempt users from the requirements of the current law and regulation. It is too soon to foresee all the changes that the technology could bring and the resulting regulatory response but national and European regulators should ensure that consumers are not negatively impacted by this evolving technology.

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

[3] FCA Business Plan 2017/2018 https://www.fca.org.uk/publication/business-plans/business-plan-2017-18.pdf

Firms providing outsourcing solutions to financial institutions must be subject to strict oversight by relevant competent authorities. Outsourcing should not in any way have a negative impact on consumers and it is important to have clear lines of regulatory oversight and responsibility between various national supervisors (see response to 2.4). In case of an incident the liability should lie with the financial organisation and that organisation should also be the consumer's point of contact for submitting and processing a complaint.

2.10 Are the existing outsourcing requirements in financial services legislation sufficient? Who is responsible for the activity of external providers and how are they supervised? Please specify, in which areas further action is needed and what such action should be.

The current regulatory framework, especially the General Data Protection Regulation, sets out good principles to address the risks stemming from Big Data and out-sourcing. However, the increasing complexity of Big Data analytics and its effect on market outcomes will require further clarification in the specific area of financial services.

It is not clear whether consumers have a right of redress against firms making use of inaccurate or misleading data. The creator and submitter of the data may not be a financial services firm and may therefore be outside the jurisdiction of the regulator and the relevant ADR scheme. The EBA could explore making the user of data liable for any inaccuracies. This would encourage firms to check the quality of the data they use.

It would be helpful to find a way to introduce infallible data watermarking to enable traceability of data.

2.11 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?

n/a

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?

To support the development of the FinTech industry across the EU, consumer redress must be embedded in the regulatory and supervisory architecture. Establishing a level-playing field across the EU in terms of redress mechanisms will facilitate the cross-border use of FinTech solutions and boost consumer confidence. Consumer trust in financial service providers is key to establishing a single market for financial services and this is especially the case for emerging technologies.

The Panel has long advocated for a duty of care to be placed on providers of financial services and believes that it should be embedded in future financial services legislation, including those covering Fintech solutions. The principle would impose a duty to act with reasonable care towards the customer to ensure they do not suffer unreasonable harm or loss and allow national regulators to better protect the interest of consumers across the EU. A similar principle was recently introduced in EU legislation through the Insurance Distribution Directive. This legislation requires all insurance distributors to 'act honestly, fairly and professionally in the best interests of their customers'. The Panel strongly supports this principle and believes similar provisions in future FinTech related legislation would help the sector to develop and bring benefits to consumers.

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

There are clear opportunities for industry associated with Fintech, but it is good consumer outcomes which will ultimately determine whether the initiative is a success. Consumer confidence is key to the take up of Fintech solutions, especially on a pan-EU level. Business models of FinTech companies should aim at improving financial consumer experiences and facilitate financial inclusion.

For FinTech to become a success story in the EU, regulators should work where to boost consumer confidence in the sector by ensuring consumer protection is at the heart of the legislation governing FinTech.

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

PSD2 makes it impossible to introduce any kind of contract between ASPSPs/data controllers and recipients of data or TPPs. This means that the liability regime for data misuse is weak. For ASPSPs there is a difficulty in recovering costs from payments incorrectly made by a PISP. This creates tension within the system and is likely to undermine trust in the system. In research consumers consistently report that they would first go to their bank to address any problems with data misuse and/or payments issues. There needs to be a better mechanism to ensure that data misuse cases can be dealt with between TPP and the bank.

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

n/a

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

The Panel believes that any effort to make regulatory framework 'more proportionate' should be mindful not to dilute consumer protection provisions, and indeed put the consumer interest at the heart of that framework.

3.6 Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market? To what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross-border financial transactions?

Data integrity and reliability is particularly important. Inaccurate data could cause significant detriment to both firms and consumers.

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

The technology neutral approach is designed to accommodate innovation but avoid arbitrage and unfair competition. However, there may be specific areas where DLT and other FinTech solutions do not fit the existing regulatory framework and could lead to consumer detriment. There may therefore be cases where the EU needs to consider whether rules prevent or restrict sensible development that would benefit consumers and hence whether changes may be needed.

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

The Panel believes that pooling expertise in the ESAs may be beneficial and strong consumer representation at stakeholder forum would help to integrate the consumer perspective from an early stage.

3.9 Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns? If yes, please specify how these programs should be organised?

Yes, integrating the consumer perspective will be particularly important to the EU's success as a FinTech hub in the years ahead. This 'Innovation Academy' would also be useful in building the capacity of consumer organisations through 'lessons learnt' and increased interaction at the EU level.

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

n/a

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

n/a

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

n/a

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?

n/a

3.14 Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses? What other specific measures should be taken at EU level?

n/a

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 development of the FinTech industry may not only have an impact on the prudential aspect of incumbent firms but also lead to poor conduct and consumer detriment as a result of added pressure and diminishing margins. National and European regulators should closely monitor this as the industry continues to develop.

4

4.1 How important is the free flow of data for the development of a DSM 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?

Yes, the Panel believes that service users should be entitled to fair compensation when their data is processed for commercial purposes that go beyond the agreed direct relationship.

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

n/a

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

n/a

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

n/a

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

The Panel believes that big data could help SMEs with thin credit files to access credit when they were previously excluded and had to rely on personal accounts

instead. Some firms in the UK have already begun to use transaction data to build transparent credit score-cards.

However, a key characteristic of big Data is that very wide and varied types of data are used collectively. Some firms are reported to use 15,000 data points in their credit scoring algorithm.[4] This could make it difficult to explain the rationale and process behind a particular's SME's denial of credit. There is also a question mark over how relevant all this data might be and whether it can be justified under protection legislation.

Given the above, the Panel strongly believes that the use of Big Data for calculating credit scores for SMEs should be subject to the SME's explicit consent and SMEs should be able to choose the types of data they are willing to have included in their credit assessment.

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 order to protect user integrity, the controller of the data should be the SME, not the counterparties holding the credit and financial data. The SME should decide whether it wants to share its data with alternative funding providers and have some level of discretion on what type of data it wants to share.

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?

Prescriptive rules and requirements will be outdated quickly in the cyber context, primarily as a result of the pace of change and dynamic nature of the cyber threat. Cyber security requirements therefore should be principle driven rather than focusing on detailed controls which are unlikely to remain current and which will not be applicable to all due to variance in their operation models/environments.

In thinking about cyber security, firms should consider:

- Governance & Strategy
- Identification of Information Assets
- Situational Awareness
- Protection
- Detection
- Response, Recovery and Resumption
- Testing
- Leaning and Evolving

Regulators should scale their approach to the nature, complexity and potential impact of individual firms on the overall cyber security infrastructure and impact on consumers. A 'one size fits all' approach does not work well for cyber and the Panel would encourage the commission to consider how to scale expectations to address proportionality. This may include some risk evaluation criteria to be applied to firms in order to identify those posing the highest level of cyber risk.

4

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?

According to the FCA, there are no regulatory barriers preventing financial services providers from sharing cyber threat information and intelligence within the UK; but firms can sometimes demonstrate a reluctance in this area because of commercial or cultural considerations, for example if they have never participated in information sharing forums in the past.

There are considerations around second order impacts or risks caused by information sharing that should be considered. When dealing with an intelligence and adaptive adversary, it may not be in the public interest or in the interest of the financial markets to share information widely. Information sharing networks need to be tightly controlled and secured to prevent unauthorised access to or disclosure of information shared with trusted partners.

The only way to build information sharing networks is to address the issue of trust. Organisations should not be forced to share with untrusted parties beyond legal requirement. As soon as information is shared, the impacted organisation loses control of that information which introduces additional risks and threats to the firm. Only by building trusted networks in secure environments can regulators address the information sharing issues.

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)?

Penetration testing is a critical element of a cyber-security framework. However, there is concern that traditional penetration testing is no longer enough to provide the assurances that are needed by organisations in the face of today's growing threat environment. The FCA has argued that penetration tests should now be intelligence led, and focus on the relationships between the attackers (red team) and network defenders (blue team). In the UK, the FCA has established the CBEST programme with the Bank of England to provide minimum requirements for penetration testing and intelligence providers. These include a minimum of 10,000 hours financial services experience and full and ongoing accreditation by the UK Council for Registered and Ethical Security Testers (CREST). We consider that, due to the high risk nature of penetration testing on live systems, these minimum criteria are essential.

Testing scenarios should be developed relevant to the threat intelligence available and the scope and scale of the test (i.e. multi-jurisdictional vs. critical functions only). Threat Intelligence should validate who is seeking to harm a firm (threat actors), how this harm will be carried out (attack path) and detail the rationale behind these actors targeting the firm (motivation). This intelligence should inform the actions of the penetration testers who should seek to replicate the actions of these identified actors to provide a realistic testing experience and derive maximum value from penetration testing activities.

EU Coordination is essential in this space. Cross-Border collaboration may be required to understand and agree on the minimum criteria for these tests, which will involve significant logistical effort.

4.10 What other applications of new technologies to financial services, beyond those above mentioned, can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing? Are there any regulatory requirements impending them?

n/a