Trans Atlantic Consumer Dialogue

COORDINATED BY CONSUMERS INTERNATIONAL

European Commission Consultation
FinTech – A more competitive and innovative European Financial Sector

Response of the Transatlantic Consumer Dialogue (TACD)

15 June 2017

1. Fostering access to financial services for consumers and businesses

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.

On-line investment platforms are heavily promoted to consumers and we expect substantial uptake in the upcoming years. We welcome new entrants in the advice market, which is currently not adequately meeting the needs of consumers. Automated advice models hold a potential promise of better delivering transparent & accessible & cost-effective advice to the mass market segment.

Our first assessment is that such platforms have the potential to give value to consumers, by providing easier access to low-cost investment funds.

However, we have also noted that there are substantial challenges in this new market which, if not mitigated, could lead to serious detriment:

FinTech companies appear to be focused mostly on young, urban, tech-savvy, affluent customer segments which are the ones most likely to benefit from these new services.[1] FinTech companies cherry-picking the most lucrative customer segments may lead to underserving everybody else.

- Blurring boundaries between advice and execution-only services
- Cost transparency is not achieved: a study from the UK Financial Services Consumer Panel found that only 1 out of 15 consumers was able to calculate the correct amount of fees on a 1000 EUR investment[2]
- No rules for the "online journey": there should be rules on how a platform should deal with conflicting answers in the on-line questionnaire (assessing the risk-profile of the consumer)

We can see similar challenges arising in the segment of insurance-based investment products.

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, as algorithms and artificial intelligence play an increasing role in firms' decision making, they will profoundly impact consumers in the world of finance. Supervisory insight and oversight of these

[1] See the Ernst & Young Fintech Adoption Index, accessible at: http://www.ey.com/gl/en/industries/financial-services/ey-fintech-adoption-index

[2] UK Financial Services Consumer Panel position paper, accessible at: https://www.fs-cp.org.uk/sites/default/files/final_panel_position_paper_online_investment_and_advice_services.pdf

technologies will be essential to avoid massive consumer detriment.

In the retail investment area, a badly defined algorithm could spur mis-selling on an unprecedented scale. In insurance and credit, the use of big data analytics triggers fundamental questions about fairness, privacy and exclusion.

Oversight and expertise is critical as the use of classifying and predictive algorithms in FinTech is growing and the source of error and bias which leads to discriminatory effect is often complex. For example, the data input can be biased or contain errors, and the algorithms and classification schemes and their applications can be biased and can further entrench inequality. While companies have an incentive to "get the model right," the evidence is clear that these models often produce biased and discriminatory outcomes. [3]

Consumers must also have the right to object to automated decisions that affect them, but this right should not be bypassed by getting a human to rubber stamp automated decisions. Consumers need to be able to assess which types of data have been used in calculating an offer to them.

Mandatory social impact assessments of deployed algorithms conducted by the financial services firm in combination with enhanced oversight could play an important role in putting effective consumer safeguards in place.

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)?

Big data analytics will have a profound impact on consumer outcomes in the area of retail finance.

We would like to highlight here that, in other jurisdictions, regulators have actively limited the use of certain parameters in big data analytics. US member states have restricted the use of non-risk related parameters (e.g. Web surfing behavior) in insurance underwriting.

We strongly call upon the Commission, but also the European Supervisory Authorities to investigate whether there are types of data which act against the interest of consumers and the wider society

- are not predictive/or have limited predictive value for the outcome sought
- may lead to discriminatory results against consumers based on their age, gender, race, ethnicity, income or geographic location
- may be relevant to financial credit but ethically unsafe
- must require greater disclosure and/or clearer approval (explicit consent) from the consumer
- should not be collected, nor processed for pricing or marketing purposes, from an ethical point of view, i.e. because they violate a consumer's fundamental right to privacy and/or their use has the potential to cause more harm than good for the consumer and/or society in general.

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 use of artificial intelligence and big data analytics in the FinTech sector may produce a host of interrelated consumer protection challenges and risks. The main areas we have identified are:

[3] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, (New York: Crown Publishing Group, 2016).

1. Risks to Privacy/Data Protection

Fintech companies use many new on- and offline data sources, either directly collecting data from consumers or relying on third parties, for Big Data analytics to classify consumers and to make predictions about them. Social media and mobile device uses, utility payments, or other public-record information are deployed in a myriad of ways. Sophisticated data-processing capabilities allow for more precise micro-targeting, the creation of comprehensive profiles, and the ability to act instantly on the insights gained from consumer behaviors.

Millions of data points might suggest interesting correlations between consumers' behavior (e.g. their spending habits, on-line behavior) and expected outcomes (e.g. risk of defaulting credit, risk of driving badly) but correlation does not mean causality. The power of algorithms, with built-in human biases, in predicting concrete consumer outcomes, is therefore always limited. Research has confirmed that, in the credit area, there is no link between number of defaults or arrears and the amount of data points used in the creditworthiness assessment (see Assessing the Impact of Credit Data on Preventing Over-indebtedness Contributing to Prudential Regulation and Facilitating Access to Affordable and Quality Credit, Financial Services User Group, December 2015).

Conversely, price discrimination looms around the corner. In the US, one credit card company admitted considering individual consumers who were using their cards for marriage counseling or therapy to have a bigger credit risk based on its experiences with other consumers and their repayment histories. (See report of the Federal Trade Commission on Big Data, January 2016). Overall, such big data methodologies may hide intentional or unintentional discrimination against protected classes (or vulnerable consumers), generating customer segments that are closely correlated with race, gender, ethnicity, or religion.

In addition, because of the importance of the mobile phone for accessing financial services and for paying for goods and services, consumers are particularly vulnerable regarding the exploitation of their geolocation information. Consumers' privacy is increasingly threatened by these new practices.

2. Risks to Increased and Entrenched Inequality via Granular Segmentation, Scoring and Biased Data Analysis

Perhaps the biggest risk to equity, fairness, and justice stemming from new practices in the financial services sector relates to the more granular segmentation and scoring of consumers. The new data points that are available to FinTech companies are analyzed through Big-Data algorithms. They are used to classify and score individuals using past data to make future predictions based on assigned group characteristics. Assigning individuals to socially constructed classifications and then making inferences about them based on those group profiles are likely to have consequences that are not well understood and may be detrimental. There is a real risk that these methods could result in biased and discriminatory outcomes: the data input can be biased or contain errors, and the algorithms and classification schemes and their applications can be biased and can further entrench inequality. Overall, such big data methodologies may hide intentional or unintentional discrimination against protected classes (or vulnerable consumers), generating customer segments that are closely correlated with race, gender, ethnicity, or religion.

3. Price Discrimination

Big-Data practices also allow firms with pricing power to identify the highest price a consumer is willing to pay for a good or service and charge accordingly. The practice upends the current distribution of wealth by allowing firms to charge the highest possible prices to everyone.

4. Unfair and Deceptive Marketing Practices

Financial services companies, including leading banks and FinTech companies, use many of the latest data-driven digital marketing tools. This includes the use of data-driven targeting platforms that make decisions in 200 milliseconds whether and how to target an individual, and tracking that consumer across all the devices she may use. Along with alluring and personalized interactive applications, consumer are identified and targeted in real time. Fintech companies are using Facebook, Instagram, and other digital behavioral data that combine data and interactive experiences to deepen their knowledge about the user and to influence consumers and their social networks. Targeted and highly personalized marketing offers can be intrusive and foster consumer behaviors that are not in the best interest of the individual, particularly when a consumer is persuaded to became over indebted (which remains a significant societal problem and should be considered in any rule making). User persuasion profiles' where estimates of how different people respond to different triggers are developed and may be deployed. Some have described this as a new source of market failure where companies have an incentive to utilize cognitive biases to shape consumer perceptions and actions. Regulators must aim to draw a clear line between informing, nudging and outright manipulation. Increasing personalization could also reduce the comparability of products, making it harder for consumers to compare one offer with another which could have an impact on market competition and consumer rights. Also, for consumer protection purposes we have to wonder how we can assess 'reasonable expectation' if products are personalized and expectations shift and a standard of reasonable expectation as a benchmark for consumer protection is difficult to establish.

Similarly, lack of transparency around the processing of data and automated algorithms may lead to increasing information asymmetries between the financial institution and the individual and thus consumers are left with less awareness and a lack of understanding and control over important financial decisions. Coupled with a perceived ease of use of these new products, opacity of the process may make it further difficult to challenge unfair marketing practices or decisions. (See also our answer to question 1.10 concerning specific insurance risks).

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?

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?

TACD response to 1.7 & **1.8** - We support 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 is necessary.

The EU current regulatory framework is not designed with this industry in mind, which spurs regulatory arbitrage and threatens investors. As crowd investors are prone to a high risk of capital loss and have very few options on secondary markets, there must be - at the very least - effective risk warning for consumers. The recently reviewed Prospectus Directive, which substantially raises the exemption thresholds for equity crowdfunding projects (up to 8 million EUR), makes this demand more pressing than ever.

Consumer organisations have already identified several problems with crowdfunding platforms. AK Wien exposed the weak disclosure practices in this area[4]. UFC-Que Choisir recently found that major crowdfunding platforms do not live up to consumer expectations[5]. They analyzed 6 platforms that offer

[4] See Austrian Federal Chamber of Labour report on Crowdfunding, April 2014, available at: http://akeuropa.eu/_includes/mods/akeu/docs/main_report_en_337.pdf

[5] See report of UFC-Que Choisir (in French): "Financement participative: Alerte sur les risques et abus", February 2017, available at: https://www.quechoisir.org/action-ufc-que-choisir-financement-participatif-alerte-sur-les-risques-et-abus-n24530/

investment opportunities to consumers and found that the platforms do not properly assess the risk of investment projects; platforms deliberately underestimate risks, while positive elements are underlined; lack of transparency on the rates of default of projects financed through those platforms; net returns are much lower than advertised by the platforms.

Due to the digital nature of this service, and the associated cross border potential, an EU framework guaranteeing minimal consumer protection standards is essential. This could equally serve the scalability of user-friendly platforms.

Regulatory efforts should focus primarily on the following aspects: clearly visible risk notices, disclosure and organizational requirements, right of cancellation, platform liability for failure to adhere to standards and/or conducting due diligence of potential investments, and investment amount caps.

The TACD wants to make clear that a self-regulatory approach, including the promotion of a voluntary transparency label without public and private enforcement, is not sufficient to give investors the much needed trust in these new type of intermediaries and risks giving a false sense of security.

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?

Tailored insurance policies and more personalised premiums could, in theory, reduce the cost for low-risk policy holders, but first experiences in pay-as-you-drive (PAYD) policies provide mixed results.

Research[6] from the Dutch consumer organisation, Consumentenbond, found that:

- PAYD premiums are substantially higher than traditional car insurance premiums but can be lowered through adopting exemplary driving practices, resulting in rebates of up to 35%;
- Average consumers with fair driving practices are mostly better off with a traditional insurance;
- Consumers with a higher risk profile (younger or older drivers) can be sometimes better off with a PAYD insurance but firms are restricting this effect by setting age limits;
- The criteria for calculating rebates remain vague and hard to comprehend – one insurer even used gamification criteria (whereby the rebate was partly based on how the policy holder drove in comparison with other policy holders);
- Privacy concerns loom and insurers also collected data which was not necessary for the calculation of the premium.

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.)?

The increasing use of big data analytics, including very sensitive data on consumers' everyday lives, poses several fundamental risks to consumers and society

[6] See report of the Dutch consumer organization, Consumentenbond (in Dutch), November 2016, available at: https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/gidsen/geldgids/2016/nummer-7---november/gg201611p20-rijstijlverzekeringen.pdf

- **Exclusion risk**: in the insurance area, the individualisation of risk profiles is bound to have fundamental implications for the principle of solidarity and risk pooling, and the potential for a very negative impact on the most vulnerable consumers. This may lead to the skimming of the insurance pool and thus raise insurance premiums for those with a less favorable profile. For instance, in the health insurance area, as seen in the United States prior to the passage of the Affordable Care Act, consumers with higher risk profiles are likely to face unacceptably high premiums for basic insurance policies or may find themselves unable to find coverage.

  Dutch consumer group Consumentenbond has already received complaints[7] from consumers barred from obtaining an insurance policy, often based on questionable data such as having a "bad" postal code.

- **The cost of privacy and the risk of privacy unravelling**: against privacy-minded consumers, unwilling to give private information (e.g. geolocation, using wearables tracking your fitness data and/or medical parameters) in exchange for a potential reduction in premiums or credit rates, will have to pay more for their privacy. Leading insurance executives seem to be keen on establishing the "no wearables = no health insurance principle", which is not only very worrying, but completely unacceptable for a society that values individual privacy. Moreover, the unravelling effect may put pressure not just on those with exemplary behavior to give up their privacy in exchange for lower costs. Consumers with 'good behaviors' will most likely at first volunteer to be monitored, but eventually even those with 'bad behavior' are likely to volunteer, in order to avoid the presumption that non-participants have something negative to hide.

- **Price optimisation**: big data supports practices whereby firms analyse and incorporate data which are not related to consumer's risk profile or their specific needs and demands. For example, over 50% of large insurers in the US take individual (on line) shopping habits or perceived tolerances for price changes into account when setting premiums for an individual consumer. Such practices, which can result in consumers with otherwise identical risks paying different prices for the same coverage, have been banned or restricted in 15 US states.[8] Similar practices could easily be introduced in the asset management and banking sector.

- **Illusion of advice**: spurred by big data analytics, offers become more and more personalized. This might give consumers the impression they are getting real advice, with all the regulatory protections attached, while in fact they are just being purely sold financial products.

- **Big brother**: the increasing use of big data with "real-time insights into consumer behavior" is the cornerstone of "surveillance capitalism" and is extremely worrying. Imagine consumers' activities being monitored 24/7, recorded and analysed for commercial purposes by financial institutions or third parties. It is already happening in the US.

See also our answer to question 1.5 concerning risks.

2. RegTech: bringing down 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

[7] See short article by the Dutch consumer organization, Consumentenbond, (in Dutch), available at: https://www.consumentenbond.nl/juridisch-advies/andere-onderwerpen/privacy-data/kredietchecks-bedrijven-screenen-klanten

[8] See report of the Federal Insurance Office, U.S. Department of Treasury on "Protection of Insurance Consumers and Access to Insurance", November 2016, available at:https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2016_FIO_Consumer_Report.pdf

development and implementation?

Financial institutions must comply with several regulatory requirements linked to on-boarding of new and existing customers. These include for instance the Know Your Customer's due diligence (KYC) and the anti-money laundering (AML).

According to RegTech providers, technology makes it possible to ensure compliance at a lower cost through process automation and information sharing.

Here are some examples:

- identification of a customer by video chat, which can make it possible to avoid requiring the customer to physically come to the bank to open a bank account when there are other reliable means of verification;
- use of biometrics that measures and analyse people’s physical and behavioral characteristics. Biometric technology can in particular be used to verify identity;
- use of face recognition algorithms;
- use of optical character recognition to analyze the codified line at the bottom of the passport and detect potential fraud.

The development of RegTech should not create new risks for the protection of customers' privacy and personal data in particular because of increased centralization of data and/or the outsourced processing of customer data. Financial regulators and financial supervisors who are not familiar with these issues should closely work with the competent authorities responsible for privacy and personal data protection.

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

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

TACD response to 2.10 & 2.11: Several actors may be involved in the data collection, aggregation, processing, and data usage, etc, especially as more and more technology companies partner with traditional financial services companies. Firms providing outsourcing services to financial institutions must be subject to oversight and be held accountable by relevant competent authorities. Lack of control in outsourcing arrangements among other things may lead to unclear allocation of liability among all the involved parties which further puts the consumer at a disadvantage. Outsourcing should never undermine consumer protection or redress mechanisms. In case of any issues or legal violations, liability vis-à-vis the consumer must always lie with their financial institution, which should also be the consumer’s contact point.

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?

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?

TACD response to 3.1 & 3.2 The TACD supports the EU institutions' efforts to promote socially responsible innovation and FinTech products and services that offer consumers real benefits. The marketplace disruptive effects brought about by FinTech providers are often welcome developments, particularly when they offer alternative products and access channels to consumers and when they put competitive pressure on incumbent market actors such as banks, insurance companies, investment service providers and financial intermediaries, to responsibly innovate, adapt to digital realities and take better care of their customers. FinTechs have in particular developed some good products in market segments where traditional providers do not live up to consumer expectations, e.g. cross-border money transfers, financial advice, etc.

Artificial barriers to market entry established by incumbent market actors should be removed. We also welcome the EU policy-makers' efforts to adapt financial services to digital developments, such as facilitating remote distribution of financial services through remote identification of customers (action 11 of the Consumer Financial Services Action Plan[9]), provided that governance, security, liability, and supervision aspects are properly addressed.

Consumer trust in financial service providers is also key to their long term success. We therefore believe that an **appropriate EU legal framework and effective public and private enforcement** can greatly contribute to the success of FinTech solutions. This would also avoid EU market fragmentation, regulatory arbitrage, and risks to market stability. FinTechs must, of course, fully comply with consumer protection legislation that applies to traditional providers. From a consumer viewpoint, it does not matter whether a financial service is provided by a bank, a non-banking payment service provider, a crowdfunding platform, or a robo-advisor. The consumer expects to have equal fair treatment at the pre-contractual, contractual, and post-contractual stages such as fair and affordable pricing, clear and non-misleading advertising and pre-contractual information; explanation of all possible risks related to the product; and efficient and effective framework for solving possible disputes that preserves full legal rights for consumers.

While FinTechs in some sectors are already regulated at the EU level, in certain other areas the existing EU legal framework should be reviewed to take account of new FinTech business models. For example, this is the case of **crowdfunding** platforms (lending- and equity-based crowdfunding). Consumers who use crowdfunding platforms may act as lenders or investors. Crowdfunding offers opportunities to both consumers and businesses: SMEs that do not have access to bank funding can fund their projects; consumers can potentially get a better return on their money, especially considering the current low interest rate environment. National legal frameworks have been adopted by some Member States (UK, FR, IT), but those national laws are light touch and don't comply with the EU market integration objective. Last year the Commission concluded that for the time being "there is no strong case for EU level policy intervention".[10]

There is a significant risk of consumer detriment if crowdfunding actors are not properly regulated. See our response to Q 1.7- 1.8.

EU legislation regulating financial advice should also be reviewed to assess whether loopholes exist with respect to robo-advisors. Currently, there is a lack of a comprehensive legal framework for advice, encompassing different segments in retail finance. Even within the retail investment area, MiFID II and IDD, there is no convergent framework. We ask the Commission to address the dire state of financial advice across financial services. In retail investment, we have also seen that in countries applying a ban on commission, fintech developments are going faster.

In addition, FinTechs should also comply with **horizontal consumer law**, such as Unfair Commercial

[9] See European Commission Consumer Financial Services Action Plan: Better Products, More Choice, March 2017, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0139

[10] See European Commission Staff Working Document "Crowdfunding in the EU Capital Markets Union", May 2016, available at: https://ec.europa.eu/info/system/files/crowdfunding-report-03052016_en.pdf

Practices Directive, Unfair Contractual Terms Directive.

Regulation versus innovation: An argument which is often used by the industry is that regulation prevents innovation. However, in practice we have observed the opposite effect. A very good illustration is provided by the EU payments legislation. The Payment Services Directive (PSD) as well as PSD2 contributed to competition by opening the EU market to non-banking payment service providers, while at the same time setting high standards of consumer protection. In the last few years, many successful EU FinTech solutions emerged in payments area.

Public enforcement: EU and national financial supervisors must deal with consumer protection effectively and independently so that an equal level of protection is offered to all EU consumers. Convergence of supervisory practices across Member States is necessary to take into account both the growing use of digitalization and the FinTechs who provide services online and remotely, including across-borders. In that context, TACD strongly advocates for setting up an EU financial consumer protection supervisor[11].

Private enforcement: To support the development of the FinTech industry across the EU, consumer redress must be embedded in the early stages of the regulatory and supervisory architecture. Establishing a level-playing field across the EU in terms of redress mechanisms will facilitate the cross-border nature of FinTech solution and boost consumer confidence. Otherwise, consumers in countries with well-established compensation and dispute resolution services (ADR) will be averse to buying products from Member States with lower standards.

3.3. 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 European Supervisory Authorities (ESAs) should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

See our response to questions 3.1 and 3.2

3.4. 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.

As already stated above, all FinTech providers must be properly regulated and supervised. FinTechs should be able to provide services across Europe based on EU passports. An indispensable pre-condition for getting the EU passport is to be subject to the EU legal framework. This is already the case for e.g. payment service providers regulated by PSD1 and PSD2.

3.5. 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 European Supervisory Authorities (ESAs) should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

Unlike traditional financial institutions, many FinTechs specialize in one or few services. Thus, their regulatory framework should be proportionate to their activity, liability and risks posed to the financial system. However, proportionality should not lead to regulatory loopholes or arbitrage.

[11] See BEUC response to the Commission consultation on the review of the European Supervisory Authorities, May 2017: http://www.beuc.eu/publications/beuc-x-2017-051_fal_beuc_position_on_esas_review.pdf

As regards consumer protection requirements, all the relevant rules applicable to traditional financial institutions should also apply to FinTech providers according to the principle of 'same services – same risks – same rules'.

3.8. 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?

3.9. 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?

3.10. 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.

TACD response to 3.8 - 3.10. The TACD is not opposed to regulatory sandboxes because they can help to foster innovation, but they must be considered an exceptional process that cannot be understood as a shortcut to avoid regulation for any given project, as this could be against the principle of creating a level playing field for all stakeholders.

Safety for consumers should be an essential criterion for admission to the sandbox. Consumers should have the same protections as they usually have. Regulators should also have the option of requesting additional protections if necessary. This is not the case everywhere. For instance, in Singapore[12] consumers participating in a sandbox experiment cannot seek help from consumer protection schemes such as the dispute resolution scheme and the deposit insurance scheme/policy owners' protection scheme. In Australia, the consumer organisations, CHOICE and the Financial Rights Legal Centre[13] have criticized the Australian Securities and Investments Commission (ASIC)'s fintech licensing exemption scheme because its reduces consumer protection, allowing new finance companies selling financial advice, credit and some insurance to operate without a license for 12 months (they just have to send ASIC a note).

At EU level, considering the integration of the financial market and to avoid regulatory arbitrage, a certain degree of homogeneity is needed in the definition of criteria to enter the sandbox, in the internal operative and interaction with regulators and, finally, in the conditions under which the exit will take place:

- A sandbox is a specific and defined part of the market. Strict limits on the types and amounts of products that qualify should be adopted by the regulator: for instance, robo advisers, digital currency wallets could generally be able to utilise the sandbox, but not lenders and fintechs working on pensions or life insurance. In addition, a sandbox should be a closed shop for private consumers, and only open to professional consumers who are well aware of the risks involved. One of most significant uses of digital technology which has emerged is the use of automated investment advice. While such services have the potential to increase access to financial advice for consumers, any measures to increase retail investor participation through such innovative distribution channels should be accompanied by appropriate safeguards and offered only to sophisticated consumers.
- To enter the sandbox, projects should be innovative, demonstrate the impossibility or high unlikelihood to be developed without a sandbox and provide clear benefits for the clients, following a case-by-case assessment.
- Once in the sandbox, the company who has entered must accept testing conditions that ensure no detriment of consumer rights, prove that the proposition will not affect the open economy,

[12] See post on Regulatory Sandboxes on the Singaporean Government website, available at: http://www.moneysense.gov.sg/Understanding-Financial-Products/Investments/Consumer-Alerts/Regulatory-Sandbox.aspx

[13] See http://financialrights.org.au/year-long-holiday-for-financial-firms-leaves-consumers-at-risk/

and must report to the regulator according to a previously agreed roadmap.

- Exiting the sandbox is a key milestone in the process, as the final objective is that the project should enter the market under clear regulatory conditions.

Projects entering a regulatory sandbox should know in advance its limitations in time (no more than 1 year) and the scope of the sandboxing environment. Once the allocated time is over, the owner of the sandbox should provide greater clarity on the application of the regulatory framework:

- the firm decides to discontinue the project because the business case is not clear or because compliance is too burdensome;
- the authorities consider that the project fits in the current regulatory framework and provide guidance on next steps to comply;
- the authorities consider that the project does not fit in the current regulatory framework and expressly forbid any similar projects.

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 EU regulators should closely monitor this as the industry continues to develop.

Incumbent firms respond to the FinTech challenge by, inter alia, cutting their legacy costs (closing down branches, reducing workforce, etc.). This fierce competition may result in financial exclusion of certain consumer groups, e.g. those who do not have a broadband internet connection, who lack the access or the knowledge to navigate easily online, elderly people, some people with disabilities (e.g., visually impaired), and those who do not trust managing their financial life online for both privacy and security reasons. Digitalisation can enhance financial inclusion of most people, but at the same time must not leave vulnerable consumers behind. It must be ensured that basic financial services remain available offline and at reasonable cost.

4. Security

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?

In the past few years, there have been several high profile cases of hacking and data theft affecting financial and non-financial firms14. New security challenges emerge with the development of FinTechs. An issue currently being debated in both the EU and the US is the following. Many FinTech providers, in the context of providing services to consumers, want to access consumers' online banking security credentials. We strongly advise against that - the consumers' personalised security credentials used to access their online banking should not be accessible to FinTechs. This is to make sure that fraudulent FinTechs could not abuse consumer confidence and defraud their money. At the same time, we do not want the banks to discriminate against FinTech services.

Therefore, the communication interface between banks and FinTechs should be harmonised at the EU/US level.

[14] See also BEUC response to EBA consultation on innovative uses of consumer data by financial institutions, Sept 2016: http://www.beuc.eu/publications/beuc-x-2016-091_fal_beuc_response_-_innovative_uses_of_consumer_data_in_fs.pdf

We fully support the position of the European Parliament which in its recent resolution on Fintech "called on the Commission to make cybersecurity the number one priority in the FinTech Action Plan, and on the European Supervisory Authorities and the European Central Bank in its banking supervision role to make it a key element of their regulatory and supervisory programmes."[15]

[15] See http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0176+0+DOC+PDF+V0//EN