

The Consumer Voice in Europe

FINTECH: A MORE COMPETITIVE AND INNOVATIVE EUROPEAN FINANCIAL SECTOR

BEUC RESPONSE TO COMMISSION CONSULTATION



Contact: Farid Aliyev & Greg Van Elsen – financialservices@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2017-073 - 15/06/2017

Why it matters to consumers

FinTech is set to have a profound impact on consumers in retail finance. While FinTech comes with opportunities, such as increased competition and new services (e.g. peer-to-peer lending, mobile payments and peer-to-peer money transfers, telematics insurances, crowdfunding), it also poses huge challenges regarding privacy, fairness and security.

Summary

BEUC acknowledges that change is in the making for consumers managing their financial life. Financial technology will have an impact on the whole supply chain of retail finance, ranging from marketing and distribution to product design. Its impact will encompass insurance, banking and retail investment markets.

Our first assessment of fintech market developments such as automated advice, crowdfunding and telematics insurance is rather mixed. Clearly, more on-line distribution has cost-cutting potential for consumers, which is especially welcome in retail investment. Consumers also value digital solutions in the area of payments.

However, the tendency to individualise financial products poses huge questions about privacy, fairness and exclusion. It blurs the boundaries between marketing and advice and makes comparison between financial products more difficult, potentially limiting competition in the process.

While change is most welcome in one of the EU's worst performing consumer market, we should not forget that FinTech also affects the regulatory framework protecting consumers. BEUC therefore calls for a digital upgrade of financial consumer protection and making sure that all FinTech providers are properly regulated at EU level. Challenges across sectors are diverse, but the biggest challenges include:

- huge privacy and fairness issues brought by big data analytics;
- a patchy advice framework unsuited for on-line and offline distribution;
- a lack of an EU framework for crowdfunding;
- a single and standardised EU-wide Application Programming Interface to enable interoperability of FinTech solutions in the area of payments.

Finally, we reiterate our longstanding call for the development of an EU framework for simple and standardised financial products. Smart algorithms might help some consumers but it will most likely leave as much consumers more confused or badly served.

1. Fostering access to financial services for consumers and businesses

Question 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 a substantial uptake in the upcoming years. BEUC welcomes new entrants in the advice market, for which the incumbents are not delivering to consumers. Automated advice models should deliver more transparent, more accessible and more cost-effective advice to the mass market.

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

Our Danish member, the Danish Consumer Council, explicitly refers to the service provided by June.dk, which offers automated portfolio management for amounts starting from 15 EUR at an all-in cost of 0.80%. This is significantly lower than traditional portfolio management offers from Danish banks.

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

- Blurring boundaries between advice and execution-only services;
- Cost transparency is not achieved: a study from our UK member the Financial Services Consumer Panel found that only 1 in 15 consumers was able to calculate the correct amount of fees on a €1,000 investment¹;
- 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.

BEUC also refers to its take on automated advice in an earlier consultation [response](#) and its [presentation](#) during the CMU roundtable organised by the Commission.

Question 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 will play an increasing role in firms' decision making they will affect consumers profoundly in finance. Supervisory insight and oversight of these technologies will be crucial to avoid massive consumer detriment.

¹https://www.fs-cp.org.uk/sites/default/files/final_panel_position_paper_online_investment_and_advice_services.pdf

In the retail investment area, a badly defined algorithm could spur mis-selling on an unprecedented scale, due to the (possible) lack of human intervention. In insurance and credit, the use of big data analytics triggers fundamental questions on fairness, privacy and exclusion.

Consumers will also have the right to (as given by the GDPR) object to automated decisions that affect them. Therefore they need to be able, for example, to assess which (types of) data have been used in calculating an offer.

Question 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?

As we have set out in detail in our earlier consultation [response](#)², 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 states have restricted the use of non-risk related parameters (e.g. 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:

- require greater disclosure and/or clearer approval (explicit consent) from the consumer;
- should not be collected, or processed, for example for pricing or marketing purposes from an ethical point of view.

As a first step, we also call for specific guidance on how the principles coined by the GDPR should be implemented in retail finance.

Question 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?

Question 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?

Investment-based crowdfunding and peer-to-peer lending platforms are supposed to give consumers direct access to a wider range of investment options. The risk hereby is that consumers may just have more options to lose their money. To meet the expectations of consumers, a clear legal framework guaranteeing consumer rights is necessary.

The 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 should be at 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.

² http://www.beuc.eu/publications/beuc-x-2017-030_qve_beuc_bigdata_esaconsultation_publication.pdf

Our members have already identified several problems with crowdfunding platforms. Our Austrian member AK Wien exposed the weak disclosure practices in this area.³ Our French member UFC-Que Choisir recently found that major crowdfunding platforms do not live up to consumer expectations.⁴ They analyzed 6 platforms that offer 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 overemphasised; lack transparency on the rates of default of projects financed through those platforms; provide lower net returns than those advertised.

Due to the digital nature of this service, and the associated cross-border potential, an EU framework guaranteeing effective consumer protection standards is essential. This could equally allow user-friendly platforms to provide their services at the EU scale.

Regulatory efforts should focus primarily on the following aspects: clearly visible risk notices, exclusion (not just disclosure) of conflicts due to sales incentives, disclosure and organisational requirements, right of cancellation and caps on the investment amount.

BEUC wants to make clear that a self-regulatory approach, including the promotion of a voluntary transparency label without public enforcement, is not an adequate tool to give investors the much needed trust in these new types of intermediaries and risks giving a false sense of security.

Question 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. However, when premiums are personalised (to the utmost), there is no risk left to share with other policy holders. The trend to personalise premiums would potentially make nonsense of insurance.

First experiences in pay-as-you-drive (PAYD) policies provide mixed results. Research⁵ from our Dutch member 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;
- Consumer 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 (where 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.

³ http://akeuropa.eu/includes/mods/akeu/docs/main_report_en_337.pdf

⁴ <https://www.quechoisir.org/action-ufc-que-choisir-financement-participatif-alerte-sur-les-risques-et-abus-n24530/>

⁵ <https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/qidsen/geldqids/2016/nummer-7--november/gg201611p20-rijstijlverzekeringen.pdf>

Question 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 consumer's everyday lives, poses several fundamental risks to consumers and society:

- **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, potentially affecting badly more vulnerable consumers. Consumers with higher risk profiles, for example in the health insurance area, might face unacceptably high premiums for basic insurance policies or may find themselves unable to find coverage.

Dutch consumer group Consumentenbond has already received complaints⁶ from consumers barred from obtaining an insurance policy, often based on questionable data such as having a "bad" postal code. German consumer organizations have been complaining for years that credit scores often are also based on irrelevant data such as a postal code⁷ or the first name of the consumer⁸, which is not disclosed to consumers.

- **The cost of privacy:** the possible discrimination against privacy-minded consumers, unwilling to give private information, for example geolocation, using wearable devices tracking your fitness data and/or medical parameters, at the expense of higher premiums or credit rates. Leading insurance executives seem to be keen on establishing the "no wearables = no health insurance principle", which is very worrying.
- **Disparate impact of big data:** millions of data points might suggest interesting correlations between consumer's behavior, for example, their spending habits, on-line behavior, geolocation, and expected outcomes, for example risk of defaulting credit, risk of driving badly. However correlation does not mean causality. The power of algorithms, with all 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 the number of defaults or arrears and the amount of data points used in the creditworthiness assessment.⁹

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.¹⁰ 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.

⁶<https://www.consumentenbond.nl/juridisch-advies/andere-onderwerpen/privacy-data/kredietchecks-bedrijven-schermen-klanten>

⁷<https://www.welt.de/finanzen/verbraucher/article13255357/Wer-am-falschen-Ort-wohnt-bekommt-keinen-Kredit.html>

⁸<https://www.welt.de/finanzen/verbraucher/article114709366/Manche-Namen-senken-Scorewert-fuer-Kreditwuerdigkeit.html>

⁹ 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, 2015.

¹⁰<https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

- **Price optimisation:** big data supports practices where firms analyse and incorporate data which are not related to the consumer's risk profile or their specific needs and demands. For example, over 50% of large insurers in the US take individual (online) 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.¹¹ 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 personalised. 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 potentially very worrying. Imagine consumers' activities being monitored 24/7, recorded and analysed for commercial purposes by financial institutions or third parties. These developments have already begun. A German based bank screens bookings in the accounts of its customers to propose a "cheaper" energy provider. Although there may also be benefits for consumers, the risk of mis-selling rises.¹²

2. Bringing down operational costs and increasing efficiency for the industry

Question 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?

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

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;
- use of biometrics that measure 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.

¹¹ https://www.treasury.gov/initiatives/fio/reports-and-notice/Document/2016_FIO_Consumer_Report.pdf

¹² <http://www.fondsprofessionell.de/news/unternehmen/headline/hypovereinsbank-hilft-per-fintech-beim-wechsel-des-stromanbieters-134080/>

The development of RegTech should not create new risks for the protection of customers' privacy and personal data in particular because of increased centralisation 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.

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

Question 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.

Firms providing outsourcing of financial services to third parties must be subject to strict oversight by relevant competent authorities. In any case, outsourcing may not undermine consumer protection and redress mechanisms. In case of an incident, liability vis-à-vis the consumer should always lie with his financial institution, which should also be the consumer's contact point.

In Germany, there are financial services that have been outsourced with a lack of oversight by authorities (through exemptions by law). Among these are shady debt collection services (invoices without legal justification)¹³, and cash on delivery (pay before you know what you get).¹⁴

See also our response to question 2.4 regarding RegTech.

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

Question 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?

Question 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?

BEUC supports the EU institutions' efforts to promote innovation in general and FinTech in particular as long as regulation of the FinTech services works well in the interest of consumers. As we have stressed on various occasions, the disruptive effect brought about by FinTech providers may be a welcome development. They offer alternative products and access channels to consumers. Furthermore, they put competitive pressure on incumbent market actors such as banks, insurance companies, investment service providers and financial intermediaries, and force them to innovate, adapt to digital realities and potentially take better care of their customers. FinTechs in particular have been growing

¹³ <https://www.verbraucherzentrale.de/inkassodienste>

¹⁴ <https://www.verbraucherzentrale.de/online-kreditvermittlung#fallenachnahme>

in market segments where traditional providers do not live up to consumer expectations, for example in 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 online distribution of financial services through remote identification of customers (action 11 of the Consumer Financial Services Action Plan¹⁵), provided that governance, security, liability, supervision aspects are properly addressed.

An **appropriate EU legal framework and effective public and private enforcement** is necessary to make FinTech solutions a success from the perspective of consumers. 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 an (equal) fair treatment at the pre-contractual, contractual and post-contractual stages such as clear and non-misleading advertising and pre-contractual information, an explanation of all possible risks related to the product, and an efficient framework for solving possible disputes.

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 for **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, who do not have access to bank funding can fund their projects, consumers can 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 and don't fit with the EU market integration objective. Last year the Commission concluded that for the time being there is "there is no strong case for EU level policy intervention."¹⁶ 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 urgently be reviewed. Currently, there is no comprehensive legal framework for advice, encompassing different segments in retail finance. Even within the retail investment area where MiFID II and IDD apply, 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.

Regarding automated portfolio management, our Danish member pointed out that there are still some infrastructure barriers which impede Danish consumers from taking full advantage of these services. As traditional banks are still in control of the securities infrastructure, so-called robo-advisors still need to collaborate with them to offer their services, rendering this service more expensive than its US counterparts.

In addition, FinTechs should also comply with **horizontal consumer law**, such as the Unfair Commercial Practices Directive or the Unfair Contract Terms Directive.

Regulation versus innovation: An argument which is often used by the industry is that regulation prevents innovation. However, in practice we observe 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

¹⁵ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0139>

¹⁶ https://ec.europa.eu/info/system/files/crowdfunding-report-03052016_en.pdf

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 to offer an equal level of protection to all EU consumers. Convergence of supervisory practices across Member States is also important taking into account the growing digitalization and FinTechs who provide services online and remotely, including across-borders. In that context, BEUC advocates the setting up of an EU financial consumer protection supervisor.¹⁷

Private enforcement: 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 mechanism will facilitate the cross-border nature of FinTech solutions and boost competition. 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.

Question 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.

See our response to questions 3.1 and 3.2

Question 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?

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 example with payment service providers regulated by PSD1 and PSD2.

Question 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.

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

¹⁷ 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.'¹⁸

Question 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?

Question 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?

Pooling expertise at the ESA level makes sense, as FinTech developments will be divergent in member states. A European perspective should be developed in the early stage of the regulatory cycle, in order to avoid a patchy framework of national initiatives. The consumer perspective should be well represented in this work stream, including a possible Innovation Academy.

Question 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?

BEUC 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 a key 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 Singapore¹⁹ 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 Centre²⁰ have criticized the Australian Securities and Investments Commission (ASIC)'s FinTech licensing exemption scheme because it 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).

¹⁸ See European Parliament's resolution on FinTech: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0176+0+DOC+XML+V0//EN>

¹⁹ <http://www.moneysense.gov.sg/Understanding-Financial-Products/Investments/Consumer-Alerts/Regulatory-Sandbox.aspx>

²⁰ <http://financialrights.org.au/year-long-holiday-for-financial-firms-leaves-consumers-at-risk/>

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 use 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 the 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 the sandbox must accept testing conditions that ensure no detriment of consumer rights, must prove that the proposition will not affect the open economy, 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 know in advance its limitations in time (no more than 1 year) and 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.

Question 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?

Standardisation and interoperability are important for competition and a level playing field between incumbent firms and FinTechs. The pending Regulatory Standards under PSD2 are a good example. More specifically it is about communication between banks and third-party payment service providers (TPPs).

We are against allowing each bank to develop their own Application Programming Interface (API) to communicate with TPPs. That would make it impossible for any Fintech to adapt its system to such a high number of applications. In other words, FinTechs would be pushed out of the market by incumbent banks because of all the different APIs. We consider that the optimal solution would be to set up a unique and single EU-wide Application Programming Interface, without the possibility of specific routines, protocols or tools. Such an API should be elaborated by a standardisation organisation.²¹

Question 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, for example 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 (visually impaired), and those who do not trust managing their financial life online for both privacy and security reasons. Digitalisation can enhance the financial inclusion of most people, but at the same should not leave vulnerable consumers behind. It must be ensured that basic financial services remain available offline and at reasonable cost.

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

Question 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 firms²². We fully agree on the importance of taking all necessary steps against potential cyber-attacks. In its recent resolution on Fintech, the European Parliament *"called on the Commission to make cybersecurity the number one priority in the FinTech Action Plan, and on the ESAs and the ECB in its banking supervision role to make it a key element of their regulatory and supervisory programmes."*²³ BEUC has not developed a detailed position on cybersecurity yet.

²¹ See BEUC letter to Commissioner Dombrovskis, 22 May 2017: http://www.beuc.eu/publications/beuc-x-2017-054_mgo_psd2_secure_communication_between_banks_and_third_party_psps.pdf

²² 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

²³ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0176+0+DOC+PDF+V0//EN>

New security challenges emerge with the development of FinTechs. An issue currently being debated at the EU level relates to the revised Payment Services Directive is the following. Third party payment services providers (TPPs), in the context of providing services to consumers, want to access consumers' online banking security credentials. We strongly advise against that - the consumer's 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.²⁴

END

²⁴ See BEUC letter to Commissioner Dombrovskis, 22 May 2017: http://www.beuc.eu/publications/beuc-x-2017-054_mgo_psd2_-_secure_communication_between_banks_and_third_party_psps.pdf



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.