

Finance Watch Extended Response

Given the restricted space to respond and constrictions to provide comments reliant for some questions only through checking a certain response, Finance Watch attaches an extended version of the response which is referred to in the relevant questions.

Question 5.1 Please explain your reasoning on your answer to question 5, and where relevant explain the necessary adaptations:

Although the response to question 5 is 'yes' there is a risk that existing issues with the current consumer protection framework that lead to discrimination and exclusion could be exacerbated by technological developments. Whilst the regulatory framework should aim at being technology neutral it should also take into account this risk.

1. "Big data"-driven algorithms as a source of discriminatory pricing/barrier to financial inclusion

Ex: non discrimination of AI and automated decision making process... How to develop an easy and efficient control scheme of these black boxes? What is the best way to avoid negative impact in the society? – A possibility is to develop objective indicators and to monitor them: e.g. a) number of credit default per type of credit/per provider – b- a measure of company's capacity to serve all types of citizens: clients' geographic distribution of each company compared to citizens geographic distribution.

Digitalisation and Big Data Analytics have the capacity to increase profiling (beyond mass use of data for increasingly targeted marketing) to allow services to better fit the personal situation of the consumer (in the best case scenario). However, currently client segmentation has a direct impact on consumer capacity to compare different offers for the financial service they are looking for. Generally only partial offers can be easily compared as obtaining the "final price" for a product requires inputting a lot of personal data, completing forms and at times waiting on a response, which is time-consuming and prevents many consumers from repeating the exercise with several different providers. This goes some way to explain an increasing use of comparison websites by certain consumers (those who are digitally literate and educated), but using these websites does not guarantee that the consumer will find the right product for their situation (this relies on the quality of the comparison websites (market coverage / method...) and consumers might need a significant amount of time and knowledge to find the best website comparison to use).

This is why we question what real benefits sophisticated client segmentation using big data analytics brings to consumers as a whole. It might be relevant to limit the number of profiles (based on a common typology) to allow effective comparison of different companies. However, we have concerns over the capacity to consumers to reap the benefits of more personalised offers. People identified as presenting low risks, who are educated and comfortable using digital tools are likely to be able to make the most of this development, but what will happen to all the others? There is a real risk that segmentation using big data analytics will increase the capacity for companies to charge higher prices to less well equipped and educated people and therefore limit their access. Given that some of these financial products are essential services, this can have negative impact at a societal level and put an end to mutualisation and socialisation of risk, which is at the core of many financial products and especially for insurance products.

This type of discrimination is more at risk of happening (to the benefit of certain players) and less at risk of being identified and supervised. Concretely, compliance is much harder to measure and enforce (with increase of unfair competition between the fair and unfair players).

On-line direct marketing strategies can be hardly identified and supervised when they explicitly target "lower risk groups" or when advertising is dynamically adapted to certain profiles. Universal insurance companies (with a well developed level of mutualisation) might be put at risk by new comers and so are only willing to insure "low risks" by offering these consumers attractive premiums. When this happens, it can reduce the possibility for the average or higher risk consumer to access affordable premiums and means that the type of risk that is being covered is not actually being mutualised.

Public authorities should be mandated to develop, in full transparency, an open-source artificial intelligence solution that would analyse consumer data and provide them with an estimate of the prices of the financial services they should expect. This solution could complement the establishment of a financial services price observatory.

Such comparison tools exist comparing different telecommunications or mortgage credit providers, but in a fully digital financial world where all products are tailored to a consumers' profile, it would be much more interesting for a consumer to know from an independent source, the price range which fits their profile, and which prices are clearly

abusive. This also raises the question over transparency of prices and the way they are displayed, since it has been shown that even harmonizing information under certain forms like APR for interest rates, does not necessarily help consumers understand whether the offer is “good” or not, or adapted to their needs/their profile.

2. Reduced access to individual information and advice

The consumer journey is very different on-line (also depending on the type of device used) when compared with the off-line experience.

Finance Watch considers the level of understanding (information disclosure / human dialogue), the capacity to make the right choice (have a clear view on the different offers/ possibilities/ have a clear view on the key criteria to make your choice), the possibility to understand the risk taken and to make an informed decision and express the consent vary significantly between on-line and off-line channels.

On-line distribution poses a challenge to effectively meeting the information and advice obligation (CCD) in the pre-contractual phase for consumer credit products, for example. This distribution process should be designed to be EFFECTIVE and to allow consumers to truly make an informed decision, which is to giving informed consent (contrary to the current box ticking disclosure method which fails to achieve this).

3. Loss of legal protection due to the lack of transparency of automated decision-making processes

Consumer protection outlined in regulation can only be effective if these rules are properly enforced. If digitalization implies a level of technology and humans means that are not affordable or accessible to competent authorities to ensure that rules are enforced, then we should not consider them to be “technology neutral”.

Question 7. Building on your experience, what are the best ways (regulatory and non-regulatory measures) for the EU to support the uptake of nascent technologies and business models relying on them while also mitigating the risks they may pose?

Please specify what are the other ways the EU could support the uptake of nascent technologies and business models relying on them while also mitigating the risks they may pose:

Finance Watch welcomes initiatives by the EU and member states to promote nascent technologies and business models that have a demonstrable, positive utility for customers and businesses, and whose attendant risks can be managed safely through regulation and responsible business practices. In all of these initiatives the role of EU and member state authorities must be clearly defined and delineated, however. EU institutions and member states may act as promoters and advisers, on the one hand, or as regulators and supervisors on the other. They cannot be both at the same time. Regulation that has been enacted, usually on the basis of a thorough review and balance of benefits and risks for all stakeholders, cannot and should not be dismantled, unilaterally and opportunistically, to accommodate emerging technologies even before their impact has been properly assessed.

This is why Finance Watch categorically rejects the concept of regulatory sandboxes. The concept of “sandboxing” ignores the fact that a technological innovation that is not capable of operating within the existing regulatory framework is, a priori, highly unlikely to deliver a balanced set of benefits and risks that would satisfy the principles that informed that regulatory framework in the first place. Conceding on the basic premise that a product or service has to function within the given regulatory environment sets a problematic precedent that suggests, in the extreme, that regulation should respond, in the first instance, to the demands of the regulated industry.

We are also skeptical of the concept of supervisory innovation hubs. We appreciate that aspiring innovators should have access to experts who can assist them in understanding, and navigating the legal and regulatory framework for the activity they are planning to undertake. We do not consider it appropriate, however, to put supervisors in the difficult position of giving advice to the same entities they are expected to supervise in due course. Apart from potentially exposing supervisors to direct lobbying in a setting that lacks adequate transparency and monitoring arrangements, advice given by supervisors to prospective applicants could also be seen as prejudging their supervisory decisions at a later stage. Advisory and supervisory functions should remain separated, preferably by assigning the advisory function to regulatory experts at another (public or private) entity that is not part of the supervisory authority, e.g. a chamber of commerce or trade association. These external regulatory experts would not be prevented from interacting with, and seeking advice from the supervisory authority but the contact between regulated entities seeking advice and their supervisors would be intermediated and any risk of compromising supervisors’ independence mitigated. If the option of locating the advisory function outside the supervisory authority is not feasible, e.g. due to a shortage of external regulatory experts or the lack of a suitable institutional platform, the supervisory authority should, at the minimum, assign the advisory function to a dedicated unit, which is

separated from the actual supervisory function by strict “Chinese Wall” arrangements and operates largely autonomously, with its own management and reporting lines.

There is, of course, ample room for regulators to provide guidance on existing legislation and regulatory standards, and for industry participants to agree on codes of conduct that encapsulate, and encourage responsible business practices. Experience shows, however, that self-regulation may be useful to supplement, but cannot replace a binding regulatory framework.

Question 9.1 Please explain your answer to question 9 and provide examples if needed:

The ‘open banking’ initiative under Directive (EU) 2015/2366 (PSD 2) requires banks to grant technology firms access to customer data, subject to customer consent. There is no reciprocal obligation for technology firms’ to provide data to banks, and other third parties with similar access to the customer data they hold. This is likely to further accelerate the concentration of EU citizens’ personal data in the hands of a small number of large, global technology firms (ROFIEG, pg. 80). The unbundling of the value chain by PSD 2, creating a range of new, lightly-regulated categories of service providers, has created opportunities for technology firms to enter the business in a way that allows them to achieve a maximum of visibility, and traction with the end customer for a minimum of regulatory oversight. Drawing on the precedent of the unbundling of the telecom industry 20-30 years ago, incumbent financial services firms run the risk of being relegated to “dumb pipes”, i.e. providers of regulated, commoditised capacity, while lucrative services are provided by others. Whereas Finance Watch supports the original intention of PSD 2 to render payment services more competitive we believe that misguided enthusiasm for “open banking” and “value chain engineering” has actually increased concentration risk, only that the likely beneficiaries are large technology firms rather than incumbents. The principle of “same activity – same risk – same regulation” is not being observed if legislators, while regulating certain activities, allow at the same time for the creation of other, less strictly or unregulated, activities that undermine the effectiveness of that very same regulatory effort. We would therefore welcome a review of PSD 2 to better align its data-sharing provisions with GDPR and caution against similar attempts at “value chain engineering” in other areas of digital financial services.

Other areas where the principle of “same activity – same risk – same regulation” is not observed are, for instance, the markets for consumer credit, peer-to-peer lending and so-called ‘payday loans’. These activities are currently conducted largely by entities that are not formally credit institutions and therefore not subject to banking-sector regulation (CRR II, CRD V, BRRD II, and others). Under the umbrella of the Consumer Credit Directive (Directive 2008/48/EC) a collection of national frameworks and regulators exist, largely in parallel and outside of the European System of Financial Supervision (ESFS). At the same time, their activities – the extension of credit to consumers – are, not substantially different from, or less risky than conventional credit extended by banks. Finally, we would highlight the market for crowdfunding, another area where the principle of “same activity – same risk – same regulation” is not applied. The proposed regulation for European Crowdfunding Services Providers (ECSPs) is a standalone regime that will be set up alongside the existing MiFIR/MiFID II framework. As with the Consumer Credit Directive, this approach appears to be informed by a mistaken interpretation of the principle of proportionality, i.e. that individual transactions are smaller, and therefore do not require the same level of regulation, in particular regarding prudential and disclosure requirements for providers. This argument is flawed: even if individual transactions are small, providers that engage in numerous transactions can become quite sizable, in particular if they operate on a pan-European scale. If crowdfunding were to become a major source of capital markets activity (which is not the case today), market participants would face a situation where the risks crowdfunding instruments may pose, to potential investors and for financial stability in general, are not regulated in the same way as they are for equivalent financial instruments that are distributed in a conventional manner (under MiFIR/MiFID II). We agree with the finding of the ROFIEG that it is currently too easy for technology firms, in particular, to gain an advantage over established, regulated institutions by engaging in regulatory arbitrage. We categorically disagree, however, with the solution proposed by the ROFIEG. Activity-based regulation is not the answer: it merely adds new layers of complexity, for no apparent gain in regulatory effectiveness; it is prone to the same intrinsic weaknesses that have beset risk-weighted capital requirements and internal risk modelling under the Basel II/III framework since the beginning; it opens up new opportunities for incumbents, in particular large, well-resourced institutions, to fine-tune the regulatory perimeter in their favour and, as a result, weaken the existing prudential framework. The current, institutional approach, by contrast, which requires certain regulated activities to be carried out through particular legal and institutional structures, subject to strict requirements and conditions (e.g. the prudential framework for commercial and investment banking, and ancillary activities) is the result of a decades-long learning process that embodies many valuable and hard-learned lessons.

Instead of discounting the institutional approach the answer to the issues highlighted above has been given

elsewhere in the ROFIEG report: the apparent regulatory inefficiencies – between EU member states, in particular – relate, to a large extent, to gaps and inconsistencies in the legal taxonomy and terminology that is used in the financial sector (ROFIEG, recs. 10 and 15). Uniform definitions of the underlying legal concepts, and better harmonisation of legislation, e.g. by further reducing national discretions, would go a long way towards closing legal loopholes and inefficiencies and restoring a level playing field for incumbents and new entrants alike.

Question 10.1 Please explain your answer to question 10 and, if necessary, please describe how the risks would emerge, decrease or increase with the higher activity of technology companies in financial services and which market participants would face these increased risks:

As stated in our response to Question 8 above, we expect technology firms to enter the EU financial services market mainly through partnerships with incumbents, with the possible exception of certain payment and transaction banking services. Some of these entrants may, in due course, proceed to engage in deposit-taking activities, e.g. to complement their payment and transaction banking services for retail customers and SMEs and to support certain lending activities, such as consumer overdrafts and working capital facilities for SMEs. At that stage we could see some degree of competition for liquidity between entrants and incumbents, both in the market for retail and SME deposits and in the wholesale market for short-term funding where technology firms could potentially fund themselves at more favourable rates than many incumbents.

Recent evidence, e.g. from China, points towards an increase in the volatility of bank deposits and short-term funding when technology firms offer alternative cash management services, such as electronic wallets, and money market funds (MMFs) that act as substitutes for savings products. EU markets are very different, however, in terms of maturity, the availability of banking services, and regulation of deposit-taking institutions. As stated above we do not currently expect technology firms to enter the EU credit markets at scale, at least not in the near term, and are therefore less concerned, at this stage, about technology firms competing in a significant way with incumbent banks for liquidity.

We are more concerned about the potential impact of technology firms as distribution channels for saving and investment products. If technology firms are successful in providing a front-end for asset managers, their role as an aggregator of demand could lead to a concentration of the customer base. If so, the interlinkages between these activities and other activities of the technology firm, notably information and communication services, such as social media, could create, or reinforce, “herding” effects, such as mass redemptions, in times of heightened volatility that may jeopardise the liquidity position of the funds they distribute, and ultimately their managers. A similar effect could occur if technology firms choose to create their own structures, such as funds of funds, to intermediate investment, especially by retail customers, into collective investment schemes offered by incumbent managers.

Based on the evidence available so far, we would expect technology firms to take a low-touch, data-driven approach, in contrast to the traditional, more relationship-driven approach of incumbent financial institutions. There is strong evidence from other areas of the financial markets that data-driven actors, such as fund managers using algorithmic trading models, behave in highly procyclical patterns, a factor that has been shown to increase systemic instability in times of crisis. Technology firms that engage in (retail and SME) lending are likely to be equally sensitive to changes in credit market sentiment and, consequently, prone to strongly procyclical behaviour. It is worth mentioning, too, that these firms’ risk models are not subject to supervisory review and vetting and, as of now, unproven throughout a full cycle. As their engagement in credit provision grows, either directly or through partnerships, so will their marginal contribution to procyclicality.

There is no doubt, in our view, that major global technology firms will become systemically important institutions in the financial markets where they are present. By virtue of their size, global customer base and the interconnectedness of their businesses, inside and outside the financial services industry, we expect them to rapidly achieve significant market share in their target segments. Given their geographically distributed business models, with very limited physical presence, and their reluctance so far to engage in regulated businesses it could become a major challenge for regulators to devise a framework that adequately manages the potential systemic risk emanating from these new entrants.

The role of technology firms as a source of operational risk also deserves particular scrutiny. This applies for both the technology firms themselves and the financial institutions that are their customers and/or partners. In recent years, financial institutions have outsourced large parts of their in-house IT services to be managed by global technology providers. They have also turned to these technology firms for the provision of cloud services in order to enable new, innovative product offerings. Many of these services support critical functions that are indispensable for the functioning of the financial institution. A major operational failure at the technology firm would have immediate, and potentially severe repercussions for the business of the financial institution. If the technology firm

holds a dominant position in providing a particular service, and that service cannot be rapidly and adequately substituted, such a failure could even trigger a systemic crisis. Conversely, technology firms providing financial services, either by themselves or through partnerships with incumbent financial services providers, are likely to be susceptible to a heightened level of operational risk due to the sheer breadth of their offering and the interconnectedness of their various services, most of which are not subject to the same regulatory standards that are applied for financial services.

Question 11. Which consumer risks do you expect to change when technology companies gain significant market share in financial services in the EU in the five upcoming years ?

Please specify which other consumer risk(s) you expect to change when technology companies gain significant market share in financial services in the EU in the five upcoming years:

1. Risk of monopolistic control, e.g. of retail payment interfaces

Finance Watch considers that the diversity of companies present on the market contributes to competitive markets, higher standards of service, and financial inclusion. This diversity allows different business models to develop, which together are better able to serve the various groups present in European society. Trends towards a more concentrated, monolithic supply-side would likely have an immediate detrimental impact on the competitiveness, customer-orientation and inclusiveness of financial services.

2. Reduced access to individual information and advice

In the area of credit, Finance Watch has concerns over whether the obligations to provide information and advice are properly fulfilled online and achieve their objectives. It is important to ensure that consumers have sufficient information and understanding to enable them to give their free consent. Similar concerns exist in the context of personal investment services for retail customers.

3. Risk of mis-selling

In the area of credit, it is important to avoid situations where consumers in difficult financial situations are being taken advantage of, particular when accessing services online. The current online distribution process seems to focus solely on providing a loan decision as quickly as possible. There is a risk here that consumers' are encouraged to make irrational purchases and decisions based on offers that target an emotional response and remove rational barriers to making a purchase or acquiring credit.

To counterbalance this risk, consumers should have instant access to budgetary and financial analysis/advice developed by the public authorities (in the general interest), which should be targeted at improving their situation.

The analysis/advice above mentioned (AI based budgeting tool) should be adjusted to the nature of the services the consumer is envisaging. Appropriate information and advice for credit but also for insurance, savings and pension products should be made available within the same approach.

4. Risk of discriminatory/predatory/prohibitive pricing, financial exclusion

Direct and indirect discrimination arising from bias in AI design, bias in the data used,... are more likely to occur than through traditional distribution processes, which might have negative impact on financial inclusion.

This type of discrimination is more likely to occur, and less likely to be detected by customers and/or supervisors. Concretely, compliance is much harder to measure and enforce (with increase of unfair competition between the fair and unfair players).

On-line direct marketing strategies can be hardly identified and supervised when they explicitly target 'lower risk groups' or when advertising is dynamically adapted to certain profiles. Universal insurance companies (with a well-developed level of mutualisation) might be put at risk by new comers and so are only willing to insure "low risks" by offering these consumers attractive premiums. When this happens, it can reduce the possibility for the average or higher risk consumer to access affordable premiums and means that the type of risk that is being covered is not actually being mutualised.

4. Lack of effective complaints and legal redress procedures

These effective consumer protection tools are much needed, but Finance Watch has concerns over their efficacy and

their user friendliness.

Question 21. In your opinion, how could the relevant EU authorities enhance coordination among different schemes in the EU?

Please specify how else could the relevant EU authorities enhance coordination among different schemes in the EU:

As mentioned in our answer to Questions 7 and 20 above, Finance Watch welcomes the creation of innovation hubs, provided that these advisory units are separated from the actual supervisory authority. We would welcome the development of guidelines, e.g. by the European Supervisory Authorities, that draw on best practice and define common standards for the organisation, funding, governance and activities of these hubs.

It is likely that member states that consider the creation of an innovation hub will have different requirements and priorities, e.g. regarding the organisation and size of that unit, and its mandate. Member states should be encouraged to define the mandate of their innovation hub(s) in a way that balances the specific requirements of their domestic financial sectors with EU-wide policy priorities. Hubs in individual member states could concentrate on specific areas to become EU-wide focal points of expertise in their field. A pan-European network, such as the European Forum for Innovation Facilitators (EFIF), could be a suitable platform for pooling complementary expertise, exchanging best practice and promoting convergence.

As mentioned in our answer to Question 9.1. above, we believe that a new Digital Finance strategy for Europe must comprise a comprehensive set of cross-sectoral safeguards to protect EU citizens' rights in the digital space. This relates, first and foremost, to the rights to privacy and the protection of personal data and for consumer rights. Close co-ordination between financial sector supervisors, data and consumer rights protection authorities is paramount and should be institutionalised, e.g. in the form of a Joint Committee comprising the European Supervisory Authorities (ESAs) and the European Data Protection Supervisor (EDPS), supported by a stakeholder group with representatives of trade bodies, civil society and consumer organisations.

Question 26: In the recent communication "A European strategy for data", the Commission is proposing measures aiming to make more data available for use in the economy and society, while keeping those who generate the data in control.

According to you, and in addition to the issues addressed in questions 27 to 46 below, do you see other measures needed to promote a well-regulated data driven financial sector in the EU and to further develop a common European data space for finance?

In its report, the ROFIEG points out that digitalisation of the EU financial sector should be informed by "fundamental European values, such as data privacy and competition" (ROFIEG, pg. 11). Finance Watch fully agrees with this statement. The rights to privacy and the protection of personal data are guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights and, in secondary legislation, primarily by the GDPR (Regulation (EU) 2016/679). It is the responsibility of the (joint) EU legislators to enact secondary legislation, such as the GDPR, that gives effect to the guarantees of the Charter and, ex-post, the prerogative of the judiciary to assess whether such legislation conforms to the Charter and the Treaties.

We disagree, therefore, with the recommendation of the ROFIEG (rec. 1) that "the European Commission should, in cooperation with the ESAs and relevant international standard-setting bodies, develop measures clarifying the circumstances under which requirements aiming at explainability and interpretability of AI and associated technologies, ... are appropriate," and "provide guidance on how to meet explainability and interpretability requirements." If such measures were to be enacted by the European Commission, on its own, they would have to take the form of delegated or implementing acts, as defined by Articles 290 and 291 TFEU. As of today, Finance Watch is not aware of a delegation or general provision in secondary law that would provide a legal basis for such a mandate.

Likewise, we disagree with the recommendation of the ROFIEG (rec. 25) that the European Data Protection Board (EDPB) should issue general “guidance on the application of the GDPR and other relevant legislation in relation to the innovative use of technology in financial services.” In the absence of specific secondary legislation that governs fundamental issues related to the use of AI, both generally and in connection with financial services we doubt that such a mandate for the EDPB would be compatible with the strict limits on the delegation of discretionary powers imposed by the ECJ (e.g. Meroni, C559/14, EU:C:2016:349).

As stated previously (see our responses to Q.5.1 and 6.1) Finance Watch believes that the deployment of AI-enabled decision-support systems

We note that the application of GDPR in the field of financial services has been less than satisfactory so far, e.g. in the case of the Payment Services Directive (Directive (EU) 2015/2366, PSD 2) where the opinion provided by the EDPB on the topics of “explicit consent” and the protection of “silent parties” is, at the very least, debatable.

We consider that, as long as personal data collected by companies are not put easily under the control of each citizen, GDPR efficiency will be highly compromised. Citizens are the only one who should be entitled to decide to who and for what purpose he/she will provide an access (precise perimeter /duration /...) to his/her set of personal data (necessary and minimized) as regard any decision to access a financial service.

In the current model, the company – and not the user - owns the personal data. Furthermore, all the data is centrally owned by only a few bigtech companies, which became data monopolists. This is neither beneficial for users of digital services nor for competitors nor society.

The Bank for International Settlement (2019, p. 20) has recognised this problem, albeit from a competition point of view alone, and proposes to assign property rights on private data to customers: “The issue, therefore, is how to promote data-sharing. Currently, data ownership is rarely clearly assigned. For practical purposes, the default outcome is that big techs have de facto ownership of customer data, and customers cannot (easily) grant competitors access to their relevant information. This uneven playing field between customers and service providers can be remedied somewhat by assigning data property rights to the customers. Customers could then decide with which providers to share or sell data. In effect, this attempts to resolve inefficiencies through the allocation of property rights and the creation of a competitive market for data – the decentralised or “Coasian” solution.”

Assigning property rights over personal data to the individual implies the creation of the individual’s self-determined digital identity. Personal attributes, such as colour of skin, DNA, name, age, fingerprint etc. constitute the digital identity of the individual. If the individual has full control of his or her private data, they become the sovereign of their own data and should decide for themselves when to collect, disclose and share the data with others. Therefore, the human right to privacy is contingent on the right to generate one’s own identity.”

While this question seems to focus only on data made available by the customer to the financial service provider, a much deeper digital finance revolution could happen if data held by the financial service providers was made available to the wider public. For instance, if Member States or the EU would require all financial service providers to make public a certain number of data points or collect certain data points and make them publicly available, this could have a major incidence on consumer behaviour for the better. For instance, every financial service provider would have to share what his level of non-performing loans is broken down by product in order to have a granular overview of the “quality” of the various products. Statistics about complaints from clients should also be publicly available. Each Member State could then develop a centralized tool which processes all that data and gives key information to consumers every time they intend to purchase a certain product such as:

What is the default rate of that product compared to the industry’s average?

How many consumers have issued complaints about the product compared to the industry’s average?

Such information could be key in order to measure how risky a product is, and its overall quality. Other data could also be interesting such as collecting data on fees related to the use of a certain product etc. Another impact will be on the general “behaviour” of the companies, which will be pushed in a virtuous cycle: publicity on bad players on the market by supervisory authorities have proven to be efficient to clean the market from bad practices (Italy, Australia...)

This “data revolution” should not only be one directional (from consumers to businesses). Consumers should also have the right to have access to more information about the business and the products they are about to purchase.

Question 42.1 Please explain your answer to question 42 and, if necessary, please explain your reasoning and provide examples:

The deployment of RegTech (including SupTech) solutions has the potential to materially increase the efficiency and effectiveness of financial sector supervision. The financial crisis of 2008 has highlighted the need for supervisors to have better, more granular access to data, ideally in real time, in order to detect, and respond to emerging crisis situations. At the same time, supervisory authorities are struggling to process the rapidly growing volumes of increasingly complex, and granular financial information produced by the institutions they supervise. The automation of regulatory reporting and supervisory processes, enabled by RegTech tools, could help solve this dilemma. RegTech tools should, in our view, be defined narrowly as software applications and algorithms that use “Big Data” analytics to process data supplied by regulated financial institutions, ideally in real time, apply relevant regulatory rules, identify potential compliance issues, and provide alerts and recommendations to supervisory staff. We believe that RegTech applications have a potentially very useful role to play as decision-support tools but should not be allowed, under any circumstances, to assume, let alone supplant the decision-making powers and responsibilities of a human supervisor or compliance officer. We do see four significant issues in this respect: firstly, the adoption of RegTech requires considerable investment from both regulated firms and supervisors; secondly, the effectiveness of RegTech and SupTech tools critically depends on the availability and quality of data; thirdly, the adoption of RegTech must not create new dependencies on dominant providers of key technology or undermine the transparency and accountability of compliance and supervisory processes; fourthly, RegTech has to be embedded in a more harmonised supervisory legal framework that does not exist yet and could prove to be very challenging to implement (see also our response to Q.44 below). The effectiveness of introducing RegTech, too, will be predicated upon the ability and readiness of financial institutions to undertake the necessary internal measures to facilitate the accurate and timely collection and consolidation of relevant data, in particular in the case of large, complex institutions. Only recently the BCBS confirmed, once again, that no global systemically important bank (G-SIB) currently conforms to the BCBS 239 standard on effective risk data aggregation and risk reporting, more than four years after its original implementation deadline (BCBS D 501, 29 April 2020). This lack of progress is, in our view, a matter of financial institutions’ priorities rather than technological feasibility: on the one hand, real-time data access for supervisors has already been trialled successfully in some smaller jurisdictions, e.g. the Philippines; on the other hand, large financial institutions appear to be perfectly prepared to invest large amounts into sophisticated IT systems, e.g. for online (retail) banking and trading, but are signally uninterested in spending money on facilitating better supervision. Legislators and regulators must lean more forcefully on financial institutions that are reluctant to invest in updating and consolidating their often fragmented and sometimes outdated IT systems. On the other end of the spectrum, we see RegTech as a potentially game-changing opportunity to level the playing field in favour of smaller market participants. RegTech-enabled automation of supervision and compliance processes could bring down the fixed cost of regulatory reporting and compliance for smaller market participants without compromising on the quality and effectiveness of regulatory oversight. In this context, Finance Watch would like to reiterate its position regarding the cost of regulatory compliance, and the need for proportionality for smaller and non-complex institutions that took place in connection with 2019 Banking Package, and the cost-benefit analysis requested from EBA in Article 430(8) CRR II: instead of considering sweeping carve-outs for small and non-complex institutions from certain reporting and other compliance obligations, EU legislators and regulators should aim at facilitating the adoption of RegTech by these institutions as a means of reducing the cost and resource-intensity of regulatory compliance. We believe that the objective of real-time supervision of financial institutions is technologically feasible for many segments of their activity and will, in due course, be financially affordable, even for smaller institutions. Financial stability is a public good and we consider it entirely reasonable to expect the financial sector to contribute its share, by investing in state-of-the-art technology, to facilitate the adequate and timely supervision of its activities. With the adoption of AI-supported systems, in particular for the purposes of predictive analytics and AI-supported or fully automated decision-making, EU legislators and regulators should also take steps to ensure that the transparency and accountability of reporting and compliance processes, on the one hand, and of supervisory decisions, on the other, are maintained. AI-supported RegTech must not become a “black box” that cannot, or only with great difficulty, be reviewed and interpreted by humans. EU legislation must ensure that management of financial institutions and supervisors remain fully accountable for all decisions made with the assistance of AI-supported RegTech systems. We are mindful that the creation of a reliable legal framework for implementing RegTech solutions is likely to be fraught with considerable legal and practical difficulty. It stands to reason that the implementation of RegTech solutions must, at all times, satisfy the fundamental preconditions of legality and due process. Legality requires that a) the functioning of any automated system (including the acquisition and processing of data, the use of legal concepts and assumptions, etc.), complies at all times, and in all its aspects, with the relevant legal norms and their interpretation and application by the courts (including higher-level concepts that may be enshrined in constitutional law or fundamental rights – see, e.g., the ECHR’s decision in the case *“Grande Stevens et al. vs. Italy”*, ECHR 062 (2014) of 04 March 2014, ECLI:CE:ECHR:2014:0304JUD001864010); and b), when a legal syllogism is applied, it is done in a transparent and methodologically correct way that conforms with legal doctrine and jurisprudence. In respect of the requirement of due process, we note that our legal context is one of

contradictory procedures between financial institutions and supervisory authorities when a rule is found to have been infringed. This has always been a very “manual” process, with exchanges of letters, lawyers, hearings, judgments, and appeals. Even if RegTech solutions are used as decision-support tools it remains imperative that administrative decisions are still made by humans, in accordance with the appropriate procedural requirements, and that courts control the process very closely, both at member state level and at European level. We note that particular care should be taken to prevent the emergence of dominant suppliers and proprietary standards in the RegTech market. There is a risk that RegTech, similar to other segments of the software and IT services market, could end up with a small number of suppliers of RegTech solutions achieving dominant market positions. Such an outcome would likely stifle competition, increase the cost for financial institutions and perhaps even hand control of reporting and compliance formats and processes to the solution provider. EU legislators and regulators should act swiftly in establishing harmonised, open standards, e.g. for data formats and interfaces (APIs) and monitor the marketplace to prevent the emergence of proprietary de-facto standards and oligopolistic market structures.