Securities and Markets Stakeholder Group

30 July 2021
ESMA22-106-3473

ADVICE TO ESMA

European Commission’s request to EBA, EIOPA and ESMA for technical advice on digital finance and related issues

Executive summary

1. The SMSG welcomes the European Commission's recent legislative proposals for the regulation of the digital finance sphere, including the Digital Finance package of September 2020. and the Digital Markets Act (DMA) of December 2020. The SMSG would like to take the opportunity of the Commission's Request for Advice to the European Supervisory Authorities, and to ESMA in particular, to express stakeholders' views and concerns.

2. Digital financial services have the potential to unlock significant benefits for financial services firms, businesses and consumers in the EU and could become an important enabling factor for the further integration and deepening of European capital markets. Insights gained from the aggregation and analysis of data using algorithms and, increasingly, so-called 'artificial intelligence' (AI), have the potential to enhance existing products and services, and enable new, innovative offerings to the benefit of businesses and consumers.

3. The SMSG notes, however, that the Commission’s approach towards ‘open finance’ and retail investments, in particular, which draws on the ‘open banking’ concept introduced for payment services by Directive (EU) 2015/2366 (PSD 2), should be carefully considered and adapted in order to avoid shortcomings, e.g. regarding consumer and data protection and the reconfiguration of the supply-side value chain, that have already become apparent in connection with that framework.

4. The SMSG observes that regulators and supervisors' assessment should be guided, at all times, by the need to preserve the standards of consumer protection established, among others, in Directive 2014/65/EU (MiFID II), and to ensure the protection and responsible handling of EU citizens' personal data, in line with Article 8 of the EU Charter of Fundamental Rights, the principles set out in Article 5 of Regulation (EU) 2016/679 (GDPR), and in the Commission's 'Digital Agenda for Europe'.

5. The SMSG points out that digitalisation has, in many instances, favoured the emergence of highly concentrated competitive outcomes. It encourages regulators and supervisors to introduce appropriate regulatory safeguards to prevent the excessive concentration of market power, in particular with respect to digital platforms, in order to maintain competitive markets and preserve financial stability.

I. Background

On 2 February 2021, the European Commission published a request to EBA, EIOPA and ESMA for technical advice on digital finance and related issues (the 'RfA'). Within the SMSG a working group has been established to provide stakeholder input to ESMA. This advice reflects the discussion of the working group as well as the consolidated comments and observations of the SMSG plenary.

II. Comments on different questions in the request for advice

1. General observations

The SMSG agrees with the Commission's overall assessment that digital innovation, and the adoption of digital services has the potential to unlock significant benefits for financial services firms, businesses and consumers in the EU and could become an important enabling factor for the further integration and deepening of European capital markets. Insights gained from the aggregation and analysis of data using algorithms and, increasingly, so-called 'artificial intelligence' (AI), have the potential to enhance existing products and services, and enable new, innovative offerings to the benefit of businesses and consumers. The SMSG notes, however, that the general principles of regulating the process of digitalisation and the use of Artificial Intelligence (AI) in financial services must be observed: legal certainty, a level playing field among providers of services, and consistently high standards of protection for retail users of digital financial services, and for citizens' personal data, in general.

The SMSG notes that the 'open banking' blueprint established for payment services in Directive 2015/2366/EU (PSD 2) (see also sec. 2.4.) does not readily lend itself as a template to be applied, with some modifications, to other areas of financial services. On the one hand, the SMSG is not convinced that the ease with which PSD 2 facilitates the commercialisation and commoditisation of citizens' personal data, and its liberal interpretation of the concept of consent, constitute 'best practice' for the protection of citizen data. We would emphasise, in this context, that data portability, which 'open banking' relies on to reduce 'lock in' effects, is not a substitute for adequate data protection. On the other hand, financial markets, and retail savings and investments, are much more diverse, and very different from the payments market, and therefore require bespoke solutions.

The SMSG is of the view that the digitalisation of financial services should follow the principle of 'same activity, same risk, same regulation'. This principle should be applied evenly to preserve, or restore, a 'level playing field' in all relevant markets, stimulate competition, and avoid granting unfair competitive advantages to individual market participants or groups of participants. The SMSG is aware that high degrees of concentration already exist in some financial markets segments, and that digitalisation frequently favours the emergence of a small number of dominant platforms. Competition policies, supervision and enforcement need to be adapted, and further enhanced, to better meet these challenges.

2. Fragmented and non-integrated value chains

Request: The ESAs are asked to (i) monitor new material developments and (ii) assess any unaddressed risks to financial stability, market integrity or consumer protection.

Points for consideration:

- Examples of growing reliance on third-party providers (e.g., for cloud computing, data analytics, risk management) to deliver investment services
- Opportunities and risks brought by these developments for firms, investors and the financial system as a whole
- Possible need for adaptations to the existing regulatory and supervisory frameworks

2.1. The SMSG is aware that the emergence of new, data-centric business models has a strong, disruptive impact on established value chains. The integration of these new entrants into established value chains, especially where they involve regulated financial services, poses challenges for regulators and supervisors, in particular when determining regulatory and supervisory perimeters, coordinating supervisory responsibilities and responses, identifying and addressing problematic concentrations of systemic risk, and preventing the leakage of personal and commercial data in increasingly complex value chains to the detriment of consumers and businesses.

2.2. For a variety of reasons – including economies of scale, network effects, and behavioural dynamics – digital markets and data-centric business models have a tendency towards producing highly concentrated outcomes. While existing value chains are broken up, and new value chains develop, opportunities arise for data-centric businesses to valorise their data repositories and fixed-asset infrastructures across an increasing number of verticals. The emergence of new, sometimes mission-critical services and infrastructures, often dominated by a small number of very large providers, has created new 'single points of failure' in the financial system. On the supply-side these include, in particular, operators of cloud services, and providers of market data, portfolio data analytics, and risk management tools.

In its February 2020 report on 'Systemic Cyber Risk'[1], the ESRB describes how a 'cybersecurity incident' – a failure or disruption an IT system, expressly not limited to malicious activity – could trigger a systemic crisis, e.g. through the manipulation of price feeds and position data. The ESRB recommends a number of 'systemic mitigants'. Some of these mitigants, such as monitoring, stress-testing and incident reporting, are reflected, at least partially, in the Commission's proposal for a Digital Operational Resilience Regulation (DORA). The SMSG supports the proposal for an EU-wide oversight framework for critical ICT third-party service providers under DORA but notes that (a) the scope of DORA is fairly narrow; and (b) the allocation of supervisory responsibility in respect of designated 'critical third-party ICT service providers' (CTPPs) is complex and requires financial supervisory authorities to take on highly technical tasks that they may not be well equipped to discharge. Regarding its scope, DORA concentrates mainly on ICT infrastructure services, such as data centres, cloud computing, software and data analytics but does not seem to cover other potentially critical services such as market data (sec. 2.3). Regarding the responsibility of the ESAs for supervising CTPPs, the SMSG notes that it would appear more germane to the remit of a dedicated organisation, e.g. the European Network and Information Security Agency (ENISA). While we understand that ENISA is expected to participate in the proposed Oversight Forum as an observer, alongside the Commission, the ESRB and the ECB, the SMSG is concerned that the supervision of CTPPs under DORA could create material overlaps with the supervision of Operators of Essential Services (OES) and Digital Service Providers (DSP) under the proposed Revised Directive on Security of Network and Information Systems (NIS 2), which could affect the effectiveness of supervision. The SMSG would therefore suggest the creation of a joint coordinating body for the oversight frameworks governing DORA and NIS 2.

2.3. The SMSG notes that other dependencies, e.g. on dominant providers of market data or risk analytics, are not yet fully explored and deserve further regulatory scrutiny. The scenarios outlined in the ESRB's report on 'Systemic Cyber Risk' confirm the impression of SMSG members that 'single points of failure' could exist in these markets. The SMSG suggests that ESMA, as part of its response to this RfA, should review potential concentration risks and systemic dependencies in this area and present its findings and recommendations to the Commission.

2.4. Sometimes the fragmentation of value chains is the result of regulatory intervention, in particular by competition authorities. In the case of PSD 2, for example, the value chain in payment services was reorganised with the express aim of breaking up entrenched structures and encouraging competition. While this particular case is outside of its immediate remit the SMSG would like to point out, on a general note, that unintended side-effects of this 'value chain engineering' approach are often difficult to

[1] European Systemic Risk Board (ESRB), Systemic Cyber Risk (Report), 19 February 2020; (https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf)

anticipate and could end up exacerbating, rather than improving, competitive imbalances in the relevant sector. The SMSG is of the view that vertical 'unbundling' of the supply-side is unlikely to produce satisfactory outcomes in a data-centric, horizontally structured sector. Other, more conventional instruments at the disposal of competition authorities are likely to be more effective and produce more predictable outcomes. In addition, given that data is widely recognised as being the key asset in the digital economy, enhancing citizens' rights over their data should provide another powerful lever for redressing the balance.

2.5. The fragmentation and restructuring of value chains in financial services also creates new risks for users of digital financial services, in particular regarding the protection of their personal data. The disclosure of personal information increases, deliberately or incidentally, with each additional participant in the value chain. As the value chain grows longer and more complex it becomes increasingly taxing, for customers and supervisors alike, to establish whether any one of the constituent parts represents an authentic service in its own right or whether it is motivated mainly by the acquisition of data for other purposes, e.g. to cross-sell other products or services (see sec. 3.3. and 4.3.).

2.6. The SMSG wishes to point out, however, that the intermediaries' chain in its current setup is likewise creating drawbacks for users of financial services, for example when it comes to the exercise of shareholders' voting rights which still, despite regulatory attempts, face obstacles resulting from too many layers in the current chain and the use of omnibus accounts. To that end, new digital technologies could improve the situation for users of financial services and contribute to the Commission's expressed aim to enhance retail investors' participation in EU capital markets.

3. Platforms and bundling of services

Request: The ESAs are asked to (i) assess the extent to which platforms operating across multiple Member States are effectively regulated and supervised, (ii) advise if EU financial services regulation and supervisory practices need to be enhanced and/or modified and (iii) assess the adequacy of current supervisory capacities.

Points for consideration:

- Examples of digital platforms in the investment industry (e.g., trading platforms, fund distribution platforms, risk management platforms, aggregators, etc.)
- Risks or issues in relation to those platforms not addressed by the existing regulatory framework
- Possible need to enhance existing supervisory skills and practices

3.1. The SMSG is aware of major digital platform providers increasing their presence in financial services. So far, the most prominent initiatives focus on the payments markets, which is outside of the scope of this group. In due course, however, investment and savings products and services that are today sold directly, or through dedicated channels, such as independent financial advisers and retail brokers, could increasingly become intermediated by digital platform providers leveraging their brand recognition, direct access to customers' devices, massive data stores and user bases, and the benefits of network effects. At present, this trend is more accentuated in non-European markets, most notably China. The SMSG expects nonetheless that major digital platform providers will continue to build up their presence in the EU financial markets and welcomes the Commission's proposal for a Digital Markets Act (DMA), which aims at regulating certain critical aspects of their activities, which would include, in particular, the intermediation of financial products and services and the provision of payment services. The DMA would invest the Commission with new monitoring, investigative, and enforcement powers, including the power to impose one off fines and periodic penalty payments to sanction anti-competitive behaviour by operators of core platform services (so-called 'gatekeepers').

3.2. Another kind of risk is the increased use of artificial intelligence (AI) in voting processes. In the US, AI is being used to provide data for voting at general meetings and it enables institutional investors to robo-vote according to pre-set instructions, or in accordance with a proxy advisor's voting policy, if the investor provides no other special instructions. Such a practice necessarily transfers fiduciary voting authority from investors to proxy advisors and consequently impacts governance and oversight of companies, as it allows investors to set their voting decisions on autopilot (set and forget). According to a study[2], 114 institutional investors voted in lockstep alignment with the two largest proxy advisors and robo-voting institutional investors in the US managed collectively more than USD 5 trillion in assets in 2020. The SEC therefore has issued guidance to make clear to institutional investors that fiduciary duties cannot be outsourced. In the EU, there do not yet exist any rules governing the use of AI in the area of vote execution or fiduciary duties and the SMSG suggests the Commission to analyse this phenomenon further, especially in view of the Green Deal.

3.3. The SMSG supports the Commission's proposal to subject 'gatekeepers' to additional scrutiny. We note, however, that the economics of two-sided platform markets where product and services are intermediated, and their impact on competition in markets for information and communication services, are known to pose a number of peculiar problems in the context of antitrust law. Methodologies and tools that are traditionally used to define markets, identify dominant market positions, and measure the impact on consumers and other market participants tend to fall short in these markets, in particular where services are offered, apparently, 'for free' and personal data tend to be priced as a wholesale commodity. Insights regarding the decisive influence of 'bounded rationality' on the behaviour of market participants, and hence the competitive dynamics of the markets, are not yet incorporated adequately into the design of competition law, and the processes and tools applied by competition authorities.

3.4. The SMSG welcomes the obligation for 'gatekeepers' to refrain from combining personal data sourced from core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services without the express consent of the user. The obligation to maintain 'data silos' is a useful starting point but does not go far enough: on the one hand, the proposal is, in our view, not sufficiently granular to prevent 'gatekeepers' from aggregating data, and compiling profiles, across different categories of financial products that are, for good reason, regulated to be sold separately, e.g. current-account banking, investment products or insurance. On the other hand, end users need to have transparency, too, in line with Article 8 of the EU Charter of Fundamental Rights and Chapter 3 of the GDPR, as to what data core platform providers collect from which sources, and how they are aggregated. Unless end users are able to inspect the data sources that are collected to assemble their profiles, and to alert the authorities in the event of a breach of the gatekeeper's obligations, it seems likely that breaches will go unnoticed and the authorities' proposed new investigation powers may remain largely toothless. The granularity of the 'silo' approach will be critical for its effectiveness, and legislators should therefore ensure that 'silo-ing' in respect of the intermediation of investment services is maintained at least at the same level of granularity as the regulated products and services themselves. Legislative action may be required to amend the list of regulated services in Annex I of Directive (MiFID II) and to update Directives (EU) 2015/1535 (Information Society Services Directive), as well as the proposed Digital Markets Act (DMA) to account for, and adequately regulate the digital intermediation of financial products and services. Users of financial products and services should be granted enhanced rights of inspection and disclosure of their personal data that are stored and processed by digital finance providers (see also Section 4.2).

4. Scope Risks of Mixed-Activity Groups (MAGs)

Request: The ESAs are asked to (i) assess whether these issues exist in sectors other than banking, (ii) analyse new emerging risks related to MAGs, (iii) assess the adequacy of current licencing practices

[2] Proxy Advisors And Market Power: A Review of Institutional Investor Robovoting, Prof. Paul Rose, The Ohio State University

and regulatory requirements and (iv) analyse the need for new supervisory coordination and cooperation arrangements (with data, competition authorities) within and outside the EU.

Points for consideration:

- Identifying MAGs offering investment services
- New risks related to MAGs (e.g. use of customer data for investment strategies and offerings, marketing and social media)
- Identifying and addressing interdependencies between the financial and non-financial parts of the group

4.1. The SMSG advises that regulators and supervisors should take a more rigorous approach towards regulating what is labelled as 'technology companies' or 'Fintech'. If applied correctly, the principle of 'technology neutrality' should ensure not only that technology-enabled new entrants are not placed at a disadvantage vis à vis incumbents but also that these new entrants conform with the same regulatory framework when providing regulated services. Although it does not directly concern financial services, the European Court of Justice's decision in the *Uber Spain* case (C-434/15, ECLI: EU:C:2017:981) confirms that it is appropriate, if not necessary, for regulatory authorities to evaluate the business model of a service provider in order to distinguish between 'pure', technology-enabled intermediation services ('information society services') and those which form part of a broader offering that encompasses key aspects of delivering a regulated service (in this case a 'transport service'). This reasoning should be applied even more stringently in respect of regulated financial services.

In financial services, mixed-activity groups are known to cause issues with properly delineating the perimeter of the regulated entity for supervisory purposes. To illustrate the potential risks caused by an overly restrictive setting of the regulatory perimeter, coupled with a readiness to exclude technology-related activities from the scope of regulated financial services, the SMSG refers to its own-initiative report on the *Wirecard* case (ESMA22-106-3194). The SMSG believes that the regulatory and supervisory shortcomings identified in this case should be addressed as part of the RfA. At the legislative level, ESMA, in conjunction with EBA and EIOPA, should consider potential approaches to refine the existing legislative framework, specifically Directive 2011/89/EU (FiCOD), and adapt the provisions governing the consolidated supervision of financial conglomerates, (mixed) financial holding companies, and other mixed-activity groups to ensure the effective supervision of digital finance groups. In analogy to Article 21b of Directive 2013/36/EU (CRD V), a revised FiCOD framework may also consider requiring service providers that are controlled by entities headquartered outside of the EU to establish an intermediate parent undertaking in the EU that comprises, and is legally responsible for all of its financial-sector activities in the EU.

At the supervisory level, the SMSG suggests that ESMA, together with its fellow ESAs, should formulate proposals for the use of supervisory convergence tools to align Member States' practices with regard to defining the supervisory perimeter and exercising consolidated supervision. The SMSG is aware that the expansion of consolidated supervision would place new demands on the resources of competent authorities and would therefore suggest that the ESAs conduct a comprehensive assessment of the adequacy of supervisory capacities in the Member States to deal with the incremental workload that comes as a direct or indirect consequence of the digitalisation of financial services.

4.2. For retail users of financial services, financial institutions' and investment firms' increased reliance on technology firms can bring a number of new risks, which can be broadly categorized around infringement of privacy, compromised data security, rising risks of fraud and scams, unfair and discriminatory use of data and data analytics, use of data that are non-transparent to both consumers and regulators and, lastly, harmful manipulation of consumer behaviour.

One major risk for consumers will be the possible infringement of privacy and data security. These two issues are intertwined and raise different kinds and degrees of concern depending on what consumer data is being accessed; how sensitive and identifiable it is; who is accessing it; whether that access is legal or illegal, and if legal, whether there should be more restrictions on use and whether consumers should be more empowered to see and reject certain kinds of use. Risks to consumers may also arise over whether and how they can give permission to third parties to access their bank account data. Consumer harm may arise from inadequate control of these permissioned-access models or, in other instances, from losing access to a service that is discontinued or removed from the market. A key concern in this space is how to establish liability in the event that consumer data is compromised, in situations where it may be unclear which entity failed to protect it.

Together with cyber-insecurity, consumers might face the related risk of rising fraud and scams. Several studies report that scams are especially harmful to vulnerable groups of consumers: increased targeting of senior customers and similar predatory patterns aim to exploit people with disabilities. Additionally, the increased risk of fraud could cause indirect harm to consumers both by raising costs and by causing some legitimate customers to be screened out and denied access to financial services – especially those with identity information that is harder to verify, such as migrants and young people.

4.3. Fairness regarding how new types of data are used might be another data-related risk for consumers. Concerns are rising that, with the availability of non-traditional data, financial companies leveraging on this new data and AI in algorithmic analysis might misuse or abuse this data to guide business decisions like targeted marketing, pricing, and whether and how people qualify to receive a financial service. Concerns are also growing about what is done with all this data, especially through artificial intelligence. AI often produces “black box” data models and decisions that cannot be readily evaluated by humans, and which may, intentionally or not, produce discriminatory or otherwise inappropriate outcomes. Issues regard both the data being analysed and the methods used to analyse it. In regard of the former, the question arises whether the data being used is accurate, and whether the data set is sufficiently large to permit analysis for the purpose at hand. While, in regard of the latter, for example AI used by robo advisors shows considerable benefits for investors, including considerably lower fees, increased accessibility, and wider availability, the underlying AI is practically unknown to the users and the processes are not bound by sufficiently clear guidelines. The SMSG therefore recommends that the ESAs consider policy actions to improve these processes, e.g. by developing more detailed guidelines on investor questionnaires, asset allocation or risk profiles based on AI. In addition, we see a need to introduce a legislative framework for AI-powered automated decision-making to ensure that it is fair, transparent and accountable to consumers. Secondly, potential harm may arise from models that are using data elements that may act as proxies for prohibited factors such as race or gender and from models’ “training data” sets that may be importing inappropriate biases due to “learning” from human decision-making that was already biased and so on. Auditability can be a particular problem for AI that involves highly confidential intellectual property. Even more basically, data scientists often warn that there is, broadly, an inverse relationship between explainability and predictiveness in AI risk and forecasting models.

4.4. Another set of concerns about fintech innovation focus on the risk of behavioural manipulation. The same technologies that can help customers better manage their finances and habits have a dark side, potentially enabling providers to induce overspending, over-borrowing, and use of inferior or more expensive products. 'Big data' analytics and other technologies can provide insights that could be exploited to take advantage of behavioural patterns and cognitive biases ('bounded rationality'). These concerns are particularly relevant in respect of vulnerable consumer groups. The SMSG calls upon ESMA, and the other ESAs, to highlight these risks and outline potential regulatory remedies as part of their response to this RfA.

This advice will be published on the Securities and Markets Stakeholder Group section of ESMA's web-site.

Adopted on 30 July 2021

Veerle Colaert
Chair
Securities and Markets Stakeholder Group

Christian M. Stiefmueller
Rapporteur