eurofinas

SPECIALISED CONSUMER CREDIT PROVIDERS IN EUROPE

Eurofinas response to the European Commission's consultation on FinTech: a more competitive and innovative European financial sector

Eurofinas is the voice of consumer credit providers at European level. As a Federation, Eurofinas brings together associations throughout Europe that represent finance houses, universal banks, specialised banks and captive finance companies of car or equipment manufacturers.

The products sold by Eurofinas members include all forms of consumer credit products such as personal loans, linked credit, credit cards and store cards. Consumer credit facilitates access to assets and services as diverse as cars, furniture, electronic appliances, education etc. **Our membership encompasses both traditional consumer credit providers offering credit in branches, through agents and at the point of sale as well as lenders with dedicated digital activities**.

In 2016, consumer credit providers that are members of Eurofinas helped support European consumption by making more than 427 billion EUR goods and services available to individuals and households, reaching 1024 billion EUR of outstandings at the end of the year[1]. In addition to the provision of consumer credit, companies represented by Eurofinas distribute a small number of insurances on an optional basis. These are simple types of insurance coverage that are available to consumers when they conclude a credit agreement.

We welcome the opportunity to respond to the European Commission's consultation on FinTech: a more competitive and innovative European financial sector. Eurofinas supports the work of the European Commission to ensure that innovative technologies are applied in order to increase the efficiency of the financial sector and to provide European consumers with improved and new financial services at a better price and with more convenience while at the same time respecting the highest standards of consumer protection and personal privacy. We trust that our comments will be taken into account and remain at the disposal of the European Commission should any further questions arise.

Advanced innovative technologies are used in a number of fields by consumer credit providers. They are used to accurately and properly evaluate risk, assess the creditworthiness of applicant borrowers and fight against financial crime. Moreover, they are also used to continuously meet their customers' expectations for new distribution channels, new and more adapted services and products.

Digital innovation is rapidly transforming our industry. New technologies, competitors as well as a shifting consumer demand bring business opportunities as much as challenges. For lenders, it is a key priority to adjust to this new landscape and to take advantage of the new technologies.

[1] Eurofinas 2016 Annual Statistical Enquiry

As stated, Eurofinas represents finance houses, universal banks, specialised banks and captive finance companies of car or equipment manufacturer. Their uptake of new technologies is very much governed by their respective business models, market conditions and customer demand. **Our response is therefore based on the experience of lenders with different business models operating under varying market conditions.**

1. Fostering access to financial services for consumers and businesses

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

Many different consumer credit providers are presently exploring and taking advantage of improved and new technologies in order to enhance processes and to better perform core activities, i.e. the safe and responsible provision of credit, to comply with regulatory requirements and to offer their customers with new and improved products as well as greater convenience.

Big Data analytics, Artificial Intelligence, machine learning, e-identity solutions and automation systems are used and considered in these efforts. These tools are particularly valuable to further improve and simplify regulatory compliance activities.

Moreover, these tools are used in order to provide consumers with a greater and more relevant experience in connection to the distribution of financial products and services, in marketing activities and in other customer engagement situations, e.g. contacts with customer services. Providers are also taking advantage of FinTech tools in order to provide their customers with improved tools for personal finance management, to gain a better understanding of their respective financial situation and to improve their financial literacy.

As identified by the Commission, the use of FinTech tools may also be beneficial to groups of applicant borrowers that often face problems accessing credit products due to lack of a traditional credit history, such as a temporarily employed person or an individual that recently has re-located to a new country. Societal changes bring forward real challenges for the safe provision of financial services and greater financial inclusion. Big Data analytics may ultimately help to overcome these obstacles.

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.

Yes, robo-advice and other forms of automated financial advice solutions are helping to reach out to more consumers. We expect these tools to grow substantially in the coming years, in particular for the customer segments which strongly prefers digital and non-personal interaction.

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, adapted oversight would be desirable.

1.4 *What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?*

Due to the essential nature of risk analysis in the financial sector and adherence to the technology neutrality principle, we believe that the minimum requirements for Artificial Intelligence driven services should correspond to the applicable sector-specific legislation covering such services and products.

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?

Due to the early application stages of such services, it is generally still too early to highlight concrete challenges and risks. However, a number of issues can already be outlined at this stage.

A number of regulatory reforms have been carried out in recent years, e.g. in connection to financial instruments, insurance distribution and mortgage credit. However, legal uncertainty exists as to how the new frameworks should and fully can be applied to automated advice tools. Advice is perceived in several different ways across jurisdictions as well as between the applicable sector-specific frameworks. Also going forward, we believe it is essential that a clear distinction is made between the provision of advice and the provision of information.

In the application of new services and technologies, it is essential for lenders to evolve together with their customers. Differences in cultural perception and technological know-how exists across the EU, affecting the willingness and ability of customers to utilise such services and tools, and the use of new innovative tools can only be built on the confidence and consent offered by consumers. The use must carefully meet customers' expectations, upholding their trust in providers' ability to justly and safely provide them with services and products.

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

N/A

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?

N/A

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?

In order to maintain the high level of consumer protection set out in applicable legislation for financial services and to avoid other risks that may arise due to information asymmetry, we believe that it is important that comparable activities are subject to the same transparency requirements, including information relating to risk factors, procedures and policies as well as fraud and anti-money laundering reporting.

1.9 Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services?

N/A

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

The use of FinTech tools, e.g. Big Data analytics, can help to refine the pricing of the various products offered to consumers. In this context, customers who previously would have been declined for a loan may now be able to obtain credit. New tools allow for the enhanced use of data for the safe provision of financial products and services to an increased number of consumers. With the improved ability to understand the situation as well as the needs of an individual potential borrower, credit and insurance products may be extended to groups of consumers that previously have been under-served as well as to consumers which are facing challenges due to their employment situation or perhaps recent relocation to a new home country for a longer or shorter period of time.

That said, there is no automatic right to credit and therefore it is essential that lenders accurately assess the risks of lending as best as they can. The further use of Big Data tools may provide for a greater accuracy and new insights in these activities and this may in turn lead to a negative outcome for certain customers to which the provision of credit could only be provided at a higher risk premium or the non-provision when this would not be in their best interest.

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

2.1 What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

Big Data analytics, Artificial Intelligence, machine learning, e-identity solutions and automation systems may prove valuable to reduce costs and to improve processes in relation to:

- Creditworthiness, risk and suitability assessments
- Anti-Money Laundering (AML) and Know-Your-Customer (KYC) procedures
- Fraud and cybercrime prevention
- Product Oversight and Governance (POG)
- Reporting and disclosure obligations

Robo-advice services can stand to automatise assistance to consumers in the online environment. Consumers can be assisted through automatic means, providing immediate assistance on initial and simple enquiries quicker and at a lower cost. Combined with the growing possibility for e-identification, the digital onboarding of new customers can be simplified, decreasing the need for staff resources in this area.

2.2 What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?

Measures taken at EU level must take a dual approach, ensuring that the existing framework is also applied to new technologies and tools while also making sure that regulatory and supervisory measures do not unnecessarily hinder innovation.

To sustain the high level of consumer protection and maintain customers' trust in new innovative technologies, it is important that all players engaging in similar activities are subject to the same frameworks as well as the same level of scrutiny independently of the chosen entity structure.

To enable the outmost uptake and development of new technologies, EU measures will play an important role. The most appropriate form will be dependent of the individual situation and technology, i.e. the development and / or adaptation of legislative measures, guidelines or standards. In this context, we believe it is important to perform a comprehensive review of all relevant legislation and supervisory approaches to ensure a consistent, innovation-friendly framework.

An adherent focus on cyber security will play an important role for the development of new tools and technologies in order to provide for the necessary confidence among market players and consumers.

The uptake and development of many FinTech tools is dependent on the forthcoming General Data Protection Regulation (GDPR). The new Regulation is an important tool for the safe processing of personal data and provides not least much necessary trust for consumers in the use of their data. In this context, we believe it is important to stress that an overly restrictive interpretation of the applicable provisions could severely limit the possibility for consumer credit providers to effectively use FinTech tools, e.g. Big Data analytics, to improve risk management activities in relation to fraud detection and prevention as well as anti-money laundering processes.

2.3 What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?

N/A

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?

As outlined above in questions 1.1 and 2.1, many different consumer credit providers are presently exploring and taking advantage of improved and new technologies in order to enhance processes and to better perform core activities, i.e. the safe and responsible provision of credit and to generally comply with regulatory requirements

Big Data analytics, Artificial Intelligence, machine learning, e-identity solutions and automation systems are all important to further improve and simplify regulatory compliance activities

As previously stated we believe it is crucial to perform a comprehensive review of all relevant legislation and supervisory approaches to ensure a continuously, consistent, innovation-friendly framework. In relation to the utilisation of RegTech tools, we believe it is important to carefully assess the existing frameworks relating to data protection, the verification of electronic identities and anti-money laundering to ensure the right balance between protection, innovation and effective data usage.

We believe it is crucial to enable the widest possible use and array of solutions and a consistent, innovation-friendly approach from supervisory authorities. It remains to be seen to what extent the private sector can utilise public e-ID systems. Also, a multitude of alternative services currently exists. It is important that such alternatives are not discriminated against as this could both hinder further innovation and the ability of providers to provide the most suitable solution in their respective markets and product segments.

However, while the eIDAS Regulation champions online solutions and transactions, face-to-face transactions are still favoured under the Anti-Money Laundering framework. Due to differing national interpretations and supervisory approaches, lenders are faced with severe inconsistencies in the ability to provide digital solutions to their customers. In some Member States, lenders may use digital solutions, e.g. webcam identification, to fulfil AML and KYC obligations. However, in other jurisdictions, such transactions are deemed high risk and it is therefore not possible to effectively offer what customers would like. Going forward, it is important to foster a consistent supervisory approach where system and tools approved by the relevant competent authorities are generally accepted for AML and KYC procedures.

In addition to tools for electronic identification and signatures, further work must be done to enable information provided by an applicant borrower (e.g. on income and employment situation) to be quickly and effectively authenticated via the improved ability to use and access relevant systems and databases.

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

Eurofinas welcomes the European Banking Authority's public consultation on the outsourcing of cloud services. It is an important initiative to provide for greater certainty in this field.

We believe that the Commission has a key role to play in the creation of a clear and proportionate framework at both EU and global level to promote a greater uptake of cloud computing solutions by financial services providers.

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

Many cloud solutions that are currently available from international providers do not meet the minimum requirements needed for European financial services providers. While significant development has taken place, the solutions differ immensely in terms of offered security and transparency. Key issues relate mainly to traceability, certification of security mechanisms as well as compliance with the relevant data protection and privacy rules.

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

Distributed Ledger Technologies (DLTs) are likely to provide for promising developments for the financial services sector as well as the greater economy. However, it also raises a wide range of issues, e.g. in relation to cyber security, consumer protection and anti-money laundering. While first use cases are possible to explore it is still too early to assess if and when commercially viable DLT solutions will be available.

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

N/A

2.9 What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

N/A

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

No, we do not consider the current framework as an obstacle to outsourcing.

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.

Yes, we consider the existing regulation to be sufficient.

2.12 Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?

N/A

3. Making the Single Market more competitive by lowering barriers to entry

3.1 Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?

In order to facilitate the implementation of FinTech solutions we believe it is important that, as the Commission is pointing out, the same activities and risks are subject to the same rules and supervision. This is of particular importance in relation to application of the frameworks covering anti-money laundering, data protection, risk, and privacy as well as consumer protection.

Moreover, lenders across the EU are subject to inconsistent approaches from national regulators and supervisors. For example, in some Member States, lenders may fulfil AML and KYC procedures with non-face-to-face solutions enabling the increasingly popular fully digital journey for consumers. However, in other jurisdictions such transactions are still unjustly considered as high-risk transactions requiring enhanced due diligence. A consistent, innovation-friendly approach is needed to enable the fullest possibly uptake of FinTech solutions, providing consumers with the fully digital journey and at the same time upholding the highest standards possible.

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?

We believe that regulators and supervisors have an important role to play in fostering the uptake and development of new technologies. However, in their respective roles it is important that they more rapidly respond to the updated reality, possibly through an increased focus and use of standards and guidelines.

Moreover, we believe it is crucial that supervisors more rapidly respond to the need to update relevant competences in relation to new and more advanced technologies. This is not only needed in order to perform purely supervisory tasks but to enable supervisors to take a wider role to foster both greater competition and collaboration between the various market players.

Due to the width of competences required in order to adequately supervise and advice in relation to services enabled by new technologies, we believe that greater cooperation and coordination between all relevant supervisory authorities should be encouraged, i.e. bringing together competences from not only financial supervisory authorities but also data protection and cyber security authorities.

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.

In our view, and as we interpret the Commission's definition of FinTech, it is important to stress that the FinTech is the use of innovative financial technology to provide financial products and services. Thus, FinTech can be utilised by all market players in the financial services sector and potential measures should reflect this.

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?

We believe that activities should be appropriately authorised and supervised independently of their legal status and jurisdictions.

A level playing field and technological neutrality are crucial aspects in this context. In relation to new providers, it is important to distinguish whether they are providing new types of services or not. If the product or service already exist in one form or another, it should fall under the existing regime.

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.

We believe that an increased focus on proportionality and flexibility is required to promote innovation and enable the greatest possible uptake on FinTech solutions. We believe that this should be done through guidelines, recommendations and flexible recommendations.

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

N/A

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

Yes, the three principles outlined by the Commission are appropriate the regulatory approach to FinTech activities. However, we believe that it should be clarified that the rules on cyber security and consumer protection should be equally applied. Minimum security requirements and a sustained high level of consumer protection are necessary in order to preserve not least consumers trust in the provision of financial services in the digital environment. Thus, the same services provided through varying technological means should be subject to the same level of minimum security requirements.

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?

It is important to stress that the approaches differ widely between national supervisors as to how they perceive their role as enabler of new technology as well as to their application of new technologies within the financial services industry.

Initiatives such as regulatory sandboxes may play an important role to encourage and capitalise on innovation relating to truly disruptive new business models and / or technologies. However, in order to achieve a greater general uptake of innovative technologies and to foster partnerships and other collaborative measures between different market players, we believe more in a wide-encompassing supportive approach by relevant supervisors. This could provide for a bigger effect than such directed measures towards a limited number of players.

The European Supervisory Authorities play an important role to monitor new innovations as well as to strive for greater supervisory convergence between national supervisors. In their role setting standards as well as developing recommendations and guidelines it is crucial that they are able to bring together and coordinate the necessary technological expertise. Coordinated measures must also be carried out together with other relevant stakeholders, e.g. the European Union Agency for Network and Information Security (ENISA), in order to achieve the comprehensive knowledge needed and to be able to develop forward-looking solutions.

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?

We believe such an initiative could provide for an important forum for exchange between relevant stakeholders and could help to enable further collaboration between different market players as well as a possibility to further exchange on common issues. Due to the width of players and interaction between different industries in FinTech, it would be important that such a measure is wide-encompassing and open for all stakeholders in FinTech.

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?

Yes, common guidelines, other high-level principles and the sharing of best practices could play an important role to achieve a more consistent framework relevant for experimentation with new and truly disruptive technologies and / or business models.

The creation of a European regulatory sandbox could prove difficult in practice. Standards still vary significantly across Europe. Dedicated actions could be undertaken for those entities in cross-border activities.

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

N/A

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

We do not think that the current level of data standardisatio is a major obstacle to outsourcing. Concrete standards relating to cybersecurity issues and Information and Communications Technology (ICT) reporting mechanisms complementing the existing frameworks could be beneficial.

3.13 In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition- friendly approach to develop these standards?

N/A

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

No, while such initiatives could be important for scientific research and public administration, we believe it is important that the EU focuses on data protection and cyber security.

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.

N/A

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

4.1 How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

We share the opinion of the European Data Protection Supervisor (EDPS) that it would be problematic “introducing the idea that people can pay with their data the same way as they do with money”. The EDPS rightfully emphasises that “fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity”.[2]

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

Distributed Ledger Technologies (DLTs) are likely to provide for promising developments for the financial services sector as well as the greater economy. However, it also raises a wide range of issues, e.g. in relation to cyber security, consumer protection and anti-money laundering. While experiments can be made, it is still too early to assess if and when commercially viable DLT solutions will be available.

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

N/A

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

DLT raises many data protection issues, as confidentiality and data privacy cannot be fully guaranteed. This issue prevalent in permission-less systems.

Replication of a whole ledger recording transactions among a range of users poses risks to data privacy. Public ledgers provide no possibility to modify previous transactions (a key property of a DLT system is that it displays the entire transaction history on a chain), thereby excluding the right to be forgotten. The ability of DLT designers to anonymise ledger entries is an important issue.

The ability to maintain the secret nature of private keys and achieve the desired security properties of public key encryption is a complex and challenging undertaking. The success of the protection of keys and cryptographic data will depend upon the strength of protocols and consensus agreements for key generation, storage, distribution, revocation, and destruction.

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

N/A

4.6 How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?

N/A

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?

Due to the use of FinTech technology, more data is being stored and processed. At the same time, cyber-attacks and other cyber-crimes are becoming more frequent and increasingly complex. Cyber-security is therefore a top priority for consumer credit providers and the wider financial services sector. In the case of security incidents, the existing framework provides for a number of overlapping reporting requirements to a variety of authorities. Applicable requirements can be found in the Security of Network and Information Systems Directive, the new Payment Service Directive, the General Data Protection Regulation as well as within the Single Supervisory Mechanism. We believe that this situation could be made more efficient by allowing for an incident to be reported to one joint responsible authority.

[2] European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, March 2017.

We would welcome a clarification on the definition of "major incident".

4.8 What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

In order to effectively fight cyber-crime activities, an increased exchange of information is necessary between businesses and supervisory authorities. However, this is presently only done in a limited extent due to a lack of joint trust and legal certainty as to the possibility to share data (also within company groups). Further actions should therefore be taken in order to bring further legal clarity on the possibility of information sharing between market players. We encourage the Commission, together with other relevant stakeholders (e.g. the European Central Bank, the ENISA, the ESAs and relevant national authorities), to have a continuous dialogue on this topic.

4.9 What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

N/A

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

N/A

Contact person

Isak Bengtzboe
Legal Adviser
+32 2 778 05 73
i.bengtzboe@eurofinas.org

Eurofinas is entered into the European Transparency Register of Interest Representatives with ID n° 83211441580-56