

EIOPA-IRSG-17-12
14 July 2017

**Response of the EIOPA Insurance and
Reinsurance Stakeholder Group (IRSG) to
European Commission's public
consultation on FinTech: a more
competitive and innovative European
financial sector**

This opinion is prepared by the Insurance and Reinsurance Stakeholder Group (IRSG) and provides high level input relating to the specific questions set out in the Commission consultation.

General comments

Fintech has potential to facilitate innovative products, lower costs, improve convenience and widen access to insurance products. However, there are also potential risks such as the risk of exclusion for some consumers and security and privacy risks associated with increased access to personal data by third parties. Generally, these will be the same as for existing insurance related products and services, and covered by existing or soon to be implemented regulation (IDD, PRIIPS, GDPR, etc). Therefore, unless specific gaps have been identified, it is advisable to monitor the potential risks identified earlier and wait for implementation of these frameworks before creating further regulation.

Fintech is still very much in development with very little data or real experience on which to draw conclusions at this stage. While it is too early to consider new regulation at this stage, steps can be taken to encourage innovation while ensuring strong consumer protection is maintained. In addition to this, ongoing monitoring is needed to identify evidence of material new risks, gaps in regulation or of barriers created by regulation.

We support the Commission's three core principles: **technology-neutrality**, so that the same rules are applied to traditionally-sold products and services as those sold digitally and so ensure innovation, suitable customer protection and a level-playing field. Second, **proportionality** so that the rules are suitable for different business models, size and activities of the regulated entities. However, it is important to note that providing proportionality does not mean compromising consumer protection. Third, **improved integrity** to ensure transparency, privacy and security for consumers.

Finally, the increasing use of big data analytics is one of the main drivers of Fintech. Therefore, we would also like to refer to the IRSGs earlier opinion¹ on specific policy challenges in that area.

Potential benefits

The development of technology applied to insurance can bring increased efficiency and reduced costs to the benefit of customers. For example:

- P2P insurance for example, can reduce costs and/or allow cover for underinsured communities. Real time reinsurance platforms give transparency and reduce costs. Certain Internet of Things (IoT) solutions can be particularly helpful both for insurers and consumers, by helping to prevent losses and therefore claims or provide early warnings to minimise damage.

¹ https://eiopa.europa.eu/Publications/Stakeholder%20Opinions/IRSG-17-05_Opinion_on_Big_Data.pdf

- Online distribution of insurance, via smart phones, tablets and computers can increase convenience reduce costs, make product information easier to access, understand and compare.
- Automated advice models using artificial intelligence hold a promise of delivering transparent, personalised and cost-effective advice, of particular benefit to the mass market segment.
- Sensor technologies, such as health monitoring devices and vehicle black-boxes allow a much deeper profiling of the individual insured thus allowing an individual approach towards the risk. Such tailored insurance policies and more personalised premiums can reduce the cost for low-risk policy holders and can encourage behaviour and lifestyles which benefits the quality of life for the policyholder while reducing the cost of claims for insurers.

Potential risks

However, along with the potential for significant benefits, the IRSG notes the following range of risks and concerns. These risks need to be monitored and any gaps in regulation addressed:

- Governance, oversight and suitability of artificial intelligence algorithms (a badly defined algorithm could create mis-selling on an unprecedented scale)
- Despite requirements for permission, we need to ensure customers fully understand how their data will be used.
- Blurring boundaries between advice and execution-only automated services. Because of the nature of automated services, it is sometimes difficult for consumers to understand whether they are transacting through an advised proposition (which carries the regulatory protection afforded to advice) or whether they are transacting via an execution-only non-advised proposition without protection.
- Exclusion risk: in the insurance area, the individualisation of risk profiles has implications for the principle of solidarity and risk pooling, potentially adversely affecting more vulnerable consumers. Consumers with higher risk profiles (e.g. in health insurance area) might face high or unaffordable premiums for basic insurance policies or may find themselves unable to find coverage.
- Possible discrimination of privacy-minded consumers, unwilling to give private information (e.g. geolocation, using wearables tracking your fitness data and/or medical parameters).
- Price optimisation: big data could support practices whereby firms analyse and use data which are not related to consumer's risk profile or their specific needs and demands.
- If not regulated appropriately, Insurtechs could lead to lower protection for consumers, for example by falling prey to data security breaches or misuse of personal data with possible knock-on loss of confidence in the wider insurance sector.

Actions to facilitate innovation

InsurTech is at an early stage of development and there are a range of actions the Commission can take to facilitate, encourage and accelerate safe innovation in the European insurance industry. The IRSG therefore encourages the Commission to consider the following:

- **Drive activity on an EU-wide solution to electronic identification and ID theft.** Customers are frustrated by the need to continually have to complete identification and verification checks to

access financial services. A digitally updated system for ID theft protection should be developed EU-wide.

- **Encourage greater data sharing, collaboration and action to tackle cyber crime.** The Commission should consider a European legal framework to combat cybercrime and to foster incident data exchange between public and private institutions.
- **Taking action on FinTech infrastructure.** To develop cohesively and avoid a fragmented approach across the EU, the Commission should consider developing an action plan on Blockchain and Cyber infrastructures. Follow through proposals for a 'Blockchain observatory'; sharing best practice and collaboration between industry and regulators is vital to ensuring Blockchain's success. In addition, the Commission could encourage the financing of blockchain infrastructure and clarify how Blockchain works in the context of existing data legislation.
- **The Commission should facilitate creation of single EU-wide standards** in certain areas to accelerate and facilitate innovation. For example, creation of a standardised set of application programming interfaces (APIs) for use with blockchains in the financial services sector.
- **Future-proof digital regulation.** Financial technology is developing at an increasingly speed, a principles based approach is required to avoid regulation being out-dated and hampering innovation.
- **Create an open dialogue with industry and consumers.** An 'Innovation Academy' comprised of FinTechs, established firms, regulators and consumer bodies should be set up to look at emerging trends; ensuring consumers are protected and innovation thrives. Encourage national supervisors/regulators to exchange information on and experiences with new regulatory tools aimed to support innovation, both at EU and international level.
- **Regulatory sandboxes should be encouraged in all member states.** While there is no need for regulation or harmonisation at this stage, information exchanges across supervisors should be encouraged to share best practice, including how to ensure consumer protection is maintained. Potential cross-border issues that may emerge could also be identified and addressed through such interaction. However, it is important that sandboxes do not intentionally or unintentionally result in lower consumer protection or solvency requirements than intended by existing regulation.
- Continue to **invest in the Digital Skills** agenda to ensure there is a pipeline of talent in areas such as Blockchain and Cyber. Continue to invest in the Digital Skills agenda to ensure there is a pipeline of talent in areas such as Blockchain and Cyber.
- Greater **sharing of data to combat fraud** by encouraging member states to establish sharing frameworks and fraud registers and promoting data sharing across member states. Enhance the sharing of data to combat fraud by encouraging member states to establish sharing frameworks and fraud registers and promoting data sharing across member states