The EU Commission’s draft Action Plan for FinTech

Jacqui Hatfield, Partner at Orrick, discusses the European Commission’s draft FinTech Action Plan for the EU, which was leaked in early February 2018; Jacqui comments on what the Action Plan gets right and its omissions.

The European Commission has put together a draft EU FinTech Action Plan, which aims to improve collaboration between FinTech participants and regulators in order to build a more competitive and innovative European financial sector. The Action Plan was leaked but this is not an issue. It is not controversial. It is balanced and concentrates on all the topical FinTech issues, including digital identification, mobile payment applications, cloud computing, big data analytics, artificial intelligence and distributed ledger technologies.

The Action Plan places cyber security as a number one priority. It advocates a three-pronged approach to cyber security, putting forward the concept of a public-private workshop geared towards analysing limitations to sharing information on various threats and how they can be tackled. It details a proposal to reach out to the European supervisory authorities (‘ESAs’) by Q1 2019 to present outlines of their financial sector supervisory approaches, as well as IT security and governance requirements, in order for the Commission to gain an all-encompassing and unifying understanding of all the approaches in the EU and to assess the need for legislative alterations. In addition, by Q4 2018 the ESAs will be expected to look into the effectiveness of a potential framework for analysing cyber attacks and threats, also specifically focussing on the EU financial sector, a process which will take into account factors such as cost.

The Commission, at the request of the EU Parliament, is right to put cyber security at the forefront of its plan. It is central to the success of all FinTech initiatives, and cyber attacks could represent a threat to the stability of the financial system. Financial services is an industry commonly considered the number one target of hackers, meaning that its approach to cyber security must be robust. The success of the revised Payment Services Directive (‘PSD2’) initiatives, for example, require robust cyber security. If there are security issues, there will be a loss of confidence and nobody will want to use the Open Banking initiatives. It is in the interest of all stakeholders that it is robust.

In addition to cyber security, the Action Plan also highlights the growing number of bespoke regulatory frameworks in place for crowdfunding across the EU and is looking to harmonise this area. This is important for the crowdfunding market as such action will prevent potential liability issues and will enable effective passporting and scaling. The Action Plan also seeks to remove obstacles hindering the use of cloud services, enabling FinTech applications with the EU blockchain initiative and building capability and knowledge among regulators and supervisors in an EU FinTech lab.

The only disappointment in the Action Plan is that whilst it mentions cryptocurrencies, it only discusses regulating this area in terms of money laundering - the AML provisions will be extended to virtual currency exchanges and wallet providers under amendments to the Fourth Anti-Money Laundering Directive. The Commission issued a warning in November 2017 in regards to ICO tokens in line with other regulators including the UK’s Financial Conduct Authority (‘FCA’) and is planning on assessing the applicability of the current EU regulatory framework in regards to cryptocurrencies and ICOs during 2018. If the EU does not lead in this area, it will mean a fragmented approach between Member States in a similar way to crowdfunding, at which point the Commission is likely to decide to harmonise. It would be beneficial for the Commission to lead in this case, for example by classifying digital currency as has been seen in the US where the Commodity Futures Trading Commission has classified Bitcoin as a commodity), and once it has sufficient knowledge, to bring out an EU position on the marketing of ICOs.

It is arguable for instance that they should be treated like equity investment crowdfunding, where the issuer is seeking to raise less than the €5 million EU Prospectus Directive level, as ICO fundraising is very similar to equity investment crowdfunding. This would require an ICO platform operator to be regulated, promotional material to be fair, clear and not misleading and retail investors in ICOs being restricted to either sophisticated investors, advised investors, high net worth investors or self certified restricted investors (individuals self certifying that they are not investing more than 10% of their net assets in illiquid investments such as those on the platform). Currently it is clear that EU Member State domestic regulators are grappling with the issue themselves and would welcome a clear steer from the EU. If not the EU, perhaps the FCA can set an example by doing this.
The Commission, at the request of the EU Parliament, is right to put cyber security at the forefront of its plan. It is central to the success of all FinTech initiatives, and cyber attacks could represent a threat to the stability of the financial system.