The International Organization of Securities Commissions (IOSCO) identified eight areas that actually constitute what is currently called “Fintech.” Such areas are payments, insurance, planning, trading and investments, blockchain, lending/crowdfunding, data and analytics, and security.

The growth of the Fintech market implies a number of relevant issues and risks from a legal perspective. In this respect, it is worth noting that financial regulation is becoming increasingly complex with major financial institutions also required to comply with different regulations in many jurisdictions. As is happening also for other sectors, the challenge for regulators remains finding the right balance between the encouragement of the emerging technologies and the need to regulate them properly. Among others, we have identified our top five legal issues that must be considered when dealing with Fintech (and new technologies), based on the European Banking Authority’s "Automatic report on the prudential risks and opportunities arising for institutions from Fintech". In this article we will only touch upon various topics; you can find a more detailed analysis in other “bites” of our newsletter, including, for instance, our post on open banking (you can read it here):

1. Data protection and cybersecurity

Fintech companies collect and process great amounts of data: this allows them to shape and customize their services in accordance with the market trends and demands. In this regard, Fintech companies must ensure compliance with data protection laws (including GDPR) and must prove to have adopted appropriate cybersecurity practices. A sound data governance is therefore of paramount importance for all parties involved. That said, there additional issues to be taken into account when dealing with large databases. If you want to know more, you can also read this post.

2. Distributed Ledger Technology and smart contracts

A “Distributed Ledger Technology” (DLT) is an amount of shared and synchronized digital data spread across multiple sites or institutions, with no central administrator or centralized data storage. A typical example of DLT is the blockchain system, which can be either public or private.

The use of DLT and smart contracts for trade finance may imply several risks from a legal and practical perspective. Sometimes DLT (such as blockchain) operates in a various jurisdictions, with conflicting regulations. By way of example, a smart contract, or more simply, a contract signed by digital means may not be enforced in all the jurisdictions involved. So, the overall legal scenario remains uncertain, despite some positive initiatives in certain jurisdictions (including Italy, and this will no doubt be addressed in our next TMT Bites issue). Furthermore, also blockchain may raise certain data protection concerns. If you want to know more, read this post!

3. Robo-advisors and legal responsibility

The concept of robo-advisor is very broad. In general terms, a robo-advisor may be considered as an online and
automated portfolio management service based on an algorithm capable to provide investment services. It is currently difficult to identify the liability between the entities involved in the robo-advisors’ activities (this is one of the most common issues related to artificial intelligence systems, see also this post): this implies serious legal risks for the institutions that rely on such robo-advisors, if a detailed assessment of their functions and operations (and consequently of the allocation of the related liabilities in the event of failures and damages arisen, based on the contributions provided by each involved party) is carried out.

4. Outsourcing core banking/payment system to the public cloud

The contract to be negotiated between a financial institution and an outsourcer (such as a cloud service provider) must comply with certain requirements (e.g. the “Recommendations on outsourcing to cloud service providers” available here), thus requiring an adequate contract management process.

In this respect, it will be fundamental to take into account the European Banks Authority’s guidelines enacted on February, 25 2019 (and available here), which will apply to all outsourcing arrangements entered into after 30 September 2019. Such guidelines aim at establishing a more harmonized framework for financial institutions, namely credit institutions and investment firms, as well as payment and electronic money institutions.

Among other things, in an outsourcing environment, failure by certain cloud service providers to provide an adequate level of transparency could result in a material legal and security risk, often with complex cross-jurisdictional implications: based on the strict connections and relationships between financial institutions (and on the connected structure of the whole financial environment), lack of transparency by even one single cloud service provider may arise systemic risks.

Given the above, financial institutions will need to assess and verify (e.g. through inspections, audits, and similar procedures) cloud service providers’ compliance with a minimum set of transparency requirements, both while negotiating the cloud service provision agreements and during their execution.

5. Biometric authentication using fingerprint recognition

The use of fingerprint authentication implies relevant legal and ICT security risks, as fingerprints can be collected without customers’ consent from the everyday objects they touch. Furthermore, legal and ICT security risks arise in connection with the possibility for fingerprints to be counterfeited by unauthorized third parties. On this point, significant legal and reputational risks could arise to financial institutions from a data protection laws perspective, which discipline (also) the processing of biometric data: should suitable security measures and processes to minimize or avoid the risk of use of counterfeited fingerprints by unauthorized third parties not be adopted, financial institutions would be considered as non-compliant with legal requirements on biometric data processing.

Therefore, financial institutions have to implement technical security measures relying on the “best industry standards” as a benchmark.

Future steps

The above are some (basic) legal issues that, when properly addressed, will allow to fully benefiting from the digital transformation and the new connected technology environment, thus creating an healthy Fintech ecosystem.

We will no doubt further update you on these topics. If you found this article interesting, and you want to learn more about Fintech, do not hesitate to contact us and… do not forget to sign up to our TMT Bites Newsletter!

This article was co-authored by Valeria Schiavo (valeria.schiavo@dentons.com).
Your Key Contacts

Giangiacomo Olivi
Partner, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com