FinTech – towards a more innovative and competitive financial sector

Executive summary

FinTech can be defined as the application of technology to financial services. It holds the promise to transform and bring efficiency gains to the financial landscape and lead to the development of new business models, innovative services and products.

A new regulatory approach is needed, and should encourage and facilitate the adoption of digital business models by financial institutions, while also addressing the consumer risks and potential stability implications of new technologies and services.

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

* * *

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: Stefano Marmo; stefano.marmo@amchameu.eu +32 (0)2 289 10 36

POSITION PAPER

3 April 2017

Introduction

FinTech – the contraction of the words 'financial' and 'technology' – refers broadly to the application of new technologies to financial services. Although the term is sometimes narrowly used to refer to start-ups developing new solutions and business models, the FinTech world also includes start-ups developing new solutions and business models alongside traditional financial institutions and mature tech companies who themselves are innovating and digitising the way they deliver financial products and services for their customers.

However, a number of barriers are restraining the digital transformation of the financial services industry. The American Chamber of Commerce to the EU (AmCham EU) therefore believes a regulatory approach is needed that encourages and facilitates the adoption of digital business models by financial institutions and the emergence of new market players, while also addressing the consumer risks and potential stability implications of new technologies and services. To this end, it is important to keep the following in mind:

- A one-size-fits-all regulatory approach is not conducive to technology innovation: any new regulatory framework should be flexible, graduated and principle-based. Oversight should be tied to scale and the risks presented.
- Importantly, new rules or guidance should take into account banks' existing authorities to develop, test and launch innovative products and services. It is also important that regulators do not implicitly limit the ability to experiment; new initiatives will not always work and that should be recognised.
- Some specific activities, such as payments, lending activities and data storage, warrant careful attention by regulators, regardless of who is engaging in the activity. The risks associated with these activities may have far reaching consequences, impacting consumers and the broader financial system (i.e. money laundering, terrorist financing, disparate impact, fraud, identity theft, unauthorized transfers, etc.).
- Regulators/supervisors should develop expertise, engage both banks and nonbank innovators, and focus frameworks on functions, not specific technologies or companies.

Facilitate technology-enabled innovation in financial services

Cloud computing

Cloud computing is a technology enabler. It allows cost reduction, flexibility and scalability to respond faster to customer requests through a better use of IT resources.

However, it is only being gradually adopted as there is a lack of clear and formal guidance that is consistent across all national financial supervisors. To date, notification and approval is required each

time a financial institution wishes to launch a cloud initiative. This increases time to market and delays the process of cloud adoption.

AmCham EU believes there is a need to facilitate cloud adoption by the financial services industry. We would welcome the harmonisation of financial supervisors' regulations and expectations in cases where services and processes are outsourced to a third-party cloud services provider.

We would welcome the development of general contract term models for specific types of cloud initiatives. This could enable early approval, taking into account cloud service providers' certifications and the findings of assessments or audits performed by the supervisors.

We believe a structured dialogue between financial supervisors, cloud service providers and financial institutions can contribute to a better understanding of the fact that storing data in the cloud can be just as secure as housing data in the organisations own servers. Furthermore, cloud services could improve the resilience and stability of the financial system because cloud services are flexible and dynamic.

It can also help clarify that the right to access and audit cloud data is more important than data location. As many financial institutions have operations across the EU and the world, we would welcome the lifting of any data localisation obligations as part of the 'free flow of data initiative' to facilitate centralised cloud data infrastructure strategies.

Blockchain

Blockchain, also known as Distributed Ledger Technology (DLT), has the potential to re-shape financial services infrastructure. DLT provides an immutable, consistent transaction protocol and data store shared across a distributed network, which may facilitate transfer of assets between parties without depending on a trusted intermediary to provide centralisation of data or workflows. The use of shared ledgers could have the greatest impact on middle and back office systems, lowering operational costs and decreasing the amount of manual reconciliation required. It could also reduce compliance costs, while providing supervisors with more accurate and faster reporting. Regulatory compliance applications of DLT and other technologies are commonly referred to as RegTech.

However, the development and deployment of blockchain technology is still in its infancy. Therefore, it is important that any regulatory approach to DLT does not implicitly limit or constrain firms' ability to test and develop DLT solutions. Further, we support a regulatory framework that treats all current and future industry participants on an equal and fair basis. As DLT-based solutions are deployed into the market, this would avoid the creation of barriers to entry that could negatively impact adoption and innovation.

The potential use cases for DLT are numerous and diverse. Any regulatory framework needs to take into account the diverse applications of DLT: the adoption of a 'one size fits all' regulatory framework for DLT is unlikely to be effective. Further, while there may be aspects of the regulatory framework relevant to DLT as a technology platform, this is distinct from applying additional requirements to an already regulated financial activity that utilises DLT. If the use of DLT poses a challenge to a particular regulation or provision within a regulatory framework, policymakers should take a pragmatic approach to rectifying this situation. The possibility of DLT challenging certain regulations

should not be viewed negatively, given that the current regulatory framework did not contemplate a technology like DLT.

As policymakers continue to engage with the industry on DLT, they should encourage interoperability between different implementations of DLT so as to ensure that new infrastructures, processes and practices do not constrain one another.

Big data

The ever-increasing ability to collect greater volumes and types of data and the rapidly evolving analytical technologies are revolutionising the way financial services firms improve their insights across customers and markets, tailor financial products and services to meet customers' needs, and open up new sources of revenue. Big data also facilitates better risk management and regulatory compliance.

However, financial firms face legal uncertainty over the use of big data. Under the General Data Protection Regulation (GDPR), personal data can only be processed under certain conditions, including on the basis of client consent or 'legitimate interests'. There is a need to bring legal certainty and transparency to when legitimate interest for processing of personal data can apply, particularly for highly regulated industries such as the financial services industry in relation to economic and/or commercial matters.

Data portability will encourage an explosion of innovation as more intuitive and tailored products are developed for consumers and small businesses. Although the GDPR includes a right to data portability, it does not impose obligations on data controllers to adopt processing systems that make this technically feasible. Therefore it is important to foster standardisation of formats for data sharing akin to the requirements for banks under the revised Payment Services Directive (PSD2) as well as promote the use of open APIs to enable customers to share their data between organisations on a cross-industry basis – including from financial services, energy and healthcare providers to social media and online market places. Data collected and generated with public funds, in particular data on climate, road safety and public health should be considered open data and therefore made available as a basis for product development, pricing, underwriting and other decisions. We would therefore support the same concepts of open data across the EU.

Adapting regulation and supervision for the FinTech world

Regulatory sandbox

New services, business models and partnerships sometimes challenge the existing regulatory framework. As a result, innovative businesses face uncertainty on how different regulations and supervisory expectations apply to them, and how authorities will interpret the rules and respond to their new business solutions.

A number of financial supervisors, including the UK Financial Conduct Authority, have introduced so-called 'regulatory sandboxes'. These are controlled environments in which both incumbents and new players can test innovative solutions in real world environments with guidance from the regulator

and the potential to do so without full compliance with applicable regulations. This approach enables a more forward-looking assessment by financial supervisors, and could ultimately lead to new regulatory and supervisory approaches.

We support the regulatory sandbox concept, especially for new entrants, and believe that, if structured correctly, it has the potential to facilitate robust dialogue between banks, non-bank FinTechs and regulators on policy barriers to partnerships or deploying innovative services/technologies. However, it is important that any such initiatives take account of firms' existing authorities and capabilities to test and innovate, allowing for voluntary participation, in order to ensure that the activity of market participants is not unintentionally hindered.

Regulation of new activities and business models

New providers of financial services usually enter the market with a different business model than incumbent players. Although their services are quite similar – they meet the same customer needs –, they are provided in different ways. For example, lending or foreign exchange marketplaces are not providers of the services themselves but organisers of the market place, reconfiguring markets and giving rise to new risks.

AmCham EU supports consistent, activities-based standards for FinTechs and emerging business models. Regardless of the type or scale of company, certain activities – i.e. payments, lending, data storage, wholesale infrastructure development – warrant the same regulatory requirements because of the significance of the associated risks (AML/KYC, terrorist financing, fair lending, privacy, unauthorized data use, operational continuity, etc.) posed to consumers and the broader financial system.

Financial and data protection supervisory collaboration

The financial industry is increasingly operating data-driven business models. Greater collaboration between data protection authorities and financial supervisors is needed to provide greater guidance and certainty as well as to ensure consistent rules on access to data across industries.

International harmonisation

FinTechs have the ability to operate across jurisdictions, as the new technologies they are implementing are not limited by geographic boundaries or a single legal and regulatory regime. New regulatory and supervisory frameworks promoted by local and regional authorities to address FinTech innovation should strive to be harmonious with existing innovation frameworks. This would mitigate the risk of regulatory arbitrage and conflicting rule sets that stymie the development of innovative products and services.

Enhancing cyber security

Cyber security standards

Regulatory approaches to cyber security should be coordinated globally. Many different supervisory authorities and regulatory bodies are looking at cyber risk and a variety of different supervisory responses have emerged. Given the borderless and increasingly interconnected digital environment, supervisory approaches to cyber security and data protection are likely to be effective and efficient if they are well coordinated and implemented consistently across regions and sectors and apply to all players. Greater harmonisation of cyber security and data protection standards is needed to overcome the fragmented supervisory approach and avoid unnecessary overlaps or potential gaps in promoting cyber security.

Cyber security standards should be principles- or risk-based, enabling a firm's risk management functions to establish cyber controls commensurate with its cyber risks. New technologies, such as the Internet of Things, artificial intelligence, blockchain and cloud computing, are magnifying the cyber security challenge. The regulatory response should not be too prescriptive and sufficiently flexible to adapt to changing technology and avoid quickly becoming obsolete.

Cyber security standards should protect data confidentiality, integrity and availability without prescribing particular methods of protection. All new regulation affecting the financial sector should be built with privacy and security considerations by design, through an early and close collaboration of regulators and supervisors with the industry.

Information and best practice sharing

Better cyber risk data collection and information sharing should be encouraged to increase cyber resilience. Sharing of cyber threat intelligence and cyber incident information will increase resilience to cyber risk. By harnessing market forces that flow from cyber insurance, policymakers can advance the widespread adoption of best practices across hundreds of thousands of large and small organisations.

AmCham EU believes that sharing of cyber intelligence between public and private entities, as well as data sharing for KYC and related purposes within same entities but between the EU and US, should be made as proactive and efficient as possible. This could happen through the establishment of common operative guidelines by the European Data Protection Board and/or Mutual Legal Assistance Treaty (MLAT).

Incident reporting

Duplicative incident requirements in the Network and Information Security (NIS) Directive, General Data Protection Regulation (GDPR), revised Payment Services Directive (PSD2) and under the European Central Bank's real-time cyber incident database for Eurozone banks, could undermine a well-coordinated response and recovery in the case of cyber incidents.

AmCham EU believes the following should be considered:

- Harmonisation of different reporting formats and procedures for cyber incident notifications;
- Aggregation in a single point of contact;
- Creation of a feedback loop mechanism to support incident;
- Fraud prevention and the establishment of an early warning system.

Regulators in each Member State should also coordinate more closely regarding incident reporting, which is required for the financial services industry. A streamlined approach for each Member State would facilitate better reporting, remediation, and customer experience. For example, there are potentially over 90 data protection and financial services regulators in Europe who might need to be notified in the event of a personal data incident.