The digital transformation of the financial services industry

Executive summary

The American Chamber of Commerce to the European Union (AmCham EU) believes digital technologies offer a unique opportunity for financial institutions to make business processes more efficient and create new products and services. They can also improve regulatory compliance, disrupt key components of the value chain and above all improve the customer experience. However, a number of barriers are restraining the digital transformation of the financial services industry. AmCham EU therefore believes a regulatory approach is needed that encourages innovative technologies and facilitates the adoption of digital business models by financial institutions.

* * *

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 2015, directly supports more than 4.3 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: Emilia Jeppsson; eje@amchameu.eu, +32 (0)2 289 10 36

POSITION PAPER

31 May 2016

Introduction

At a time of unprecedented structural change in the financial services industry, financial institutions are contending with increasing challenges, including compliance with post-crisis regulations, changing customer expectations and new competition from inside and outside the industry.

The American Chamber of Commerce to the European Union (AmCham EU) appreciates significant investments are required for financial institutions to take the full opportunity of digitisation and move towards new digital business models. We believe that public policy has an important role to play both in helping to facilitate the potentially transformative power of digital technologies as well as safeguarding consumer and investor interests as the changes take hold. Concerted action is needed to overcome barriers restraining the digital transformation of the financial services industry in Europe.

A regulatory approach that encourages innovation

In considering new rules and guidance, and taking into account current supervisory practices, AmCham EU invites policy-makers to accommodate fast-paced technological developments and innovation, while maintaining a high level of consumer protection and prudent risk management for existing and new providers of financial services.

- **Principle-based approach** – EU policy-makers should encourage synergies between different industry actors to collaborate in the development of financial technology. The traditional financial industry and new market entrants should not be hindered in developing new technologies that are promising for the financial services sector. Policy-makers and regulators should start from a position of having clear, long-term overarching principles and desired outcomes. We believe any new regulations should be technology-neutral and align with open and international standards to support innovation and competition.

- **Consistent, activities-based standards for FinTechs and emerging business models –** FinTechs should be subject to the same regulatory requirements and oversight as established financial institutions if they engage in certain activities – i.e. payments, lending, wholesale infrastructure development – as the associated risks (Anti-Money Laundering 'AML'/ Know Your Customer 'KYC', terrorist financing, fair lending, operational continuity) posed to consumers and the broader financial system are significant regardless of scale. For other activities, and emerging business models (e.g. robo-advisers), potential regulatory frameworks should be tailored, flexible and principles-based, and the intensity of oversight should be tied to scale and the risks presented.

- **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.

- **Risk-based approach** – The financial services industry should be allowed to have low-risk and low-scale experimentation with new technologies *(e.g. distributed ledger technology)* and business models. The Financial Conduct Authority's (FCA) regulatory sandbox could serve as a model for financial supervisors in other EU Member States, allowing established financial firms to voluntarily access to sandboxes in the event there is regulatory or supervisory uncertainty around a particular service or technology.

- **Use of technology for regulatory compliance** – Shared IT tools offer the potential to reduce regulatory burden while maintaining high standards. Such tools could include KYC systems, automated reporting or data analytics tools. Regulators should encourage the development of 'Regtech' by ensuring that existing regulatory frameworks will allow for innovative approaches for compliance, and potentially endorse certain standards or tools to provide clarity to the industry.

Data & Cloud

AmCham EU appreciates that big data analytics and the use of cloud services to securely process and store large volumes of data are key enablers for the digital transformation of the financial services industry.

- **Data use and ownership** – The development of innovative customised financial services depends on legal certainty for the use of big data. We believe that this requires a common and innovation-enabling understanding of key concepts such as data ownership, anonymisation and pseudo-anonymisation and unambiguous consent. The newly created European Data Protection Board should issue EU guidelines to provide legal certainty as well as ensure a harmonised interpretation of the new General Data Protection Regulation (GDPR).

- **Open data** – 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 basis for product development, pricing and underwriting decisions. We would therefore support the same concepts of open data across the EU.

- **Free flow of data** – Regulation at EU and international level should bring down barriers to the transfer of data (location and access to it) and should address intra-EU and extra-EU scenarios. Unjustified national data localisation requirements should be addressed under the legislative proposal on data localisation as part of the 'free flow of data initiative' to facilitate centralised (cloud) data infrastructure strategies. We wish to underline that the legal recognition and implementation of the EU-US Privacy Shield as well as EU model contractual clauses are needed to provide legal certainty for transatlantic data flows.

- **Cloud deployment** – Legal and regulatory concerns have limited the adoption of cloud service models by the financial industry, while national financial supervisory authorities understanding of the risks and opportunities of cloud services remain limited. In this context we would welcome a structured dialogue between financial supervisors, cloud service providers and financial institutions to create a common and clear EU supervisory approval process, through a review of

European Banking Authority (EBA) guidelines on outsourcing, to accelerate cloud deployment by the banking industry.

Cyber security

Cyber-security issues are borderless, and therefore require cooperative and coordinated action among governmental, public and private stakeholders both within the EU and globally.

- **Information sharing –** The ability of the EU banking sector, law enforcement authorities and intelligence agencies to share information to combat cybercrime and fraud is currently either limited to a national scale or even not accomplished due to data privacy constraints. We believe that the 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 through the establishment of common operative guidelines by the European Data Protection Board and/or a Mutual Legal Assistance Treaty (MLAT).

- **Incident reporting –** Duplicative incident reporting requirements in the Network and Information Security (NIS) Directive, GDPR and Payment Services Directive 2 (PSD2) could undermine a well-coordinated response and recovery in the case of cyber-incidents. We therefore believe 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 and fraud prevention; and the establishment of an early warning system. We welcome the recent pilot project launched by the European Central Bank to create a real-time cyber incident database for Eurozone banks. However we think it should apply to all EU banks.

Digital onboarding and communication

In the Digital Single Market, the EU regulatory framework should enable cross-border transactions, contractual agreements and customer communication across EU borders through digital channels.

- **System on electronic identification and trust services for electronic transactions in the internal market (eIDAS) –** Cross-border recognition of national electronic identification (eID) systems, for use of online public services, will be mandated under the eIDAS Regulation by 2018. This could provide the financial industry with an efficient and remote electronic identification and e-signature system, interoperable across Member States. AmCham EU therefore believes EU Member States should allow for private sector use of the eIDAS system in addition to other solutions that guarantee strong user authentication.

- **Electronic KYC checks –** Protection against financial crime is currently location dependent because of the lack of verifiable information available across borders. We would welcome an expansion of eIDAS to offer trust services and interoperability on a broader range of customer information, including KYC data and fraud markers, as this would facilitate financial institutions to meet anti-money laundering requirements and provide easier access to distance credit for customers.

- **Alternative identification methods –** In the absence of a national eID interoperability framework, we believe current regulations on the prevention of money laundering and terrorism financing should be reviewed to accept alternative identification methods *(e.g. biometric analysis, videocall or third party verification services)* as equivalent to face-to-face due diligence checks undertaken by financial institutions**.**

- **Paperless communication –** Legislation in relation to the communication of (pre-contractual) information to customers varies which impacts service providers' ability to implement a single delivery channel distribution. In particular, it impedes the ability for financial institutions to communicate with clients digitally. We would welcome a review of the existing regulatory framework in this context, as it would help enable innovation and digitalisation in the EU retail financial services market.

Standardisation and interoperability

Standardisation and interoperability are key to building the digital economy. Alignment with international standards is essential to ensure financial institutions remain free to use innovative technologies and services regardless of the location of the provider.

- **International standards** – While several standard-setting bodies are currently developing new technology standards for emerging and leading-edge technologies, the role of the industry-led standardisation system in developing global high-quality standards remains important. However, we believe a careful assessment is needed in order to avoid conflicting standardisation on big data, cloud and cyber security. AmCham EU therefore believes the alignment with international standards is important to ensure high-quality services while allowing the industry to develop innovative and varied solutions.

- **Interoperability** – It is our firm belief that the European Commission and Member States have a role to play in promoting interoperability as a public policy goal, helping to map new priorities and fostering companies' technology contributions to standardisation. The market-led approach has achieved enormous success and this models needs to be preserved, including in the global context. The PSD2 mandate for the EBA to set requirements for open standards for communication between banks and other payment services providers is a good example of helpful policy in this regard.

Conclusion

To enable the full digital transformation of the financial services industry, AmCham EU believes a regulatory framework that encourages innovation is needed. This may require updating existing legislation rather than creating new legislation. Whereas digital technology is potentially global in reach, regulation and supervision still remain national in practice. We would therefore welcome future EU initiatives to consider the global context.