ADVISORY GROUP
MEETING PAPER 3-E

Document: AGFSCB 38-015E
Draft: **FIRST**
Date: 13 July 2018
Source: IIF
Meeting: Kuala Lumpur, Malaysia

Timothy D. Adams
President and CEO

INSTITUTE OF INTERNATIONAL FINANCE

April 26, 2018

The Honorable Steven T. Mnuchin
Secretary of the Treasury
Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

RE: Presidential Executive Order 13772 on Core Principles for Regulating the United States Financial System – 4th Report

Dear Secretary Mnuchin:

The Institute of International Finance ("IIF")[1] welcomes the Treasury's continued efforts in support of Executive Order 13772 on Core Principles for Regulating the United States Financial System (the "Executive Order").[2] We are pleased to provide our comments on this occasion in respect of the upcoming 4th Report, on Non-Bank, Non-Insurer Financial Institutions, with the aim of contributing to a constructive policy dialogue on the difficult role of policy-makers, regulators and supervisors in ensuring a resilient and stable financial system, providing a level playing field for all participants (banks and non-banks), and fostering an innovative, secure and competitive financial market and investment climate that fully supports capital formation, economic growth, and job creation.

We appreciate that the scope of Treasury's 4th Report is extremely broad, and our comments are concentrated within that scope, specifically on technological innovation and related competition issues in the financial system. Our comments relate to informed consumer and investor choice, financial stability, and the need for an efficient regulatory structure for cross-sectoral and cross-border competition in the FinTech ecosystem[3], consistent with the Core Principles.

Accordingly, we have focused on four aspects:

1. **Regulatory and supervisory frameworks should be consistent across the new competitive environment.**

[1] The IIF is a global association of the financial services industry representing over five hundred commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks in 70 countries: www.iif.com
[2] The White House: *Presidential Executive Order 13772 on Core Principles for Regulating the United States Financial System*, February 3, 2017.
[3] The FinTech ecosystem referred to in this letter encompasses all technology-driven innovation in the provision of financial services, inclusive of small new entrants, 'BigTech' companies, incumbent financial institutions and the regulators and supervisors

The principle of 'same activity, same risk, same rules, same supervision' should be the foundation of any framework in this rapidly evolving digital marketplace. In the digital space, where boundaries across sectors are fading, the regulatory and supervisory frameworks should focus on the activity undertaken and the risk it brings for customers and financial stability, and not exclusively on the nature of the entity.

This approach merits looking beyond the traditional "silos" of regulation – both within the traditional financial sector (e.g. bank regulation distinct from insurers, distinct from securities companies), and between those and broader topics such as competition policy, data protection and cyber-security. A consistent **cross-sectorial** approach is needed, where the prevailing lens is that of support of those participating in the economy, whether as investors or borrowers, rather than on the entity-type of the provider.

Furthermore, the nature of digital competition is inherently global by nature. New and emerging technological players in financial services, particularly the so-called 'BigTechs', each already have or will soon have a reach that is exceeding the local and even regional borders. This reiterates the criticality of **cross-border regulatory coordination**, as rightly highlighted in Treasury's earlier Executive Order reports. Just as a more cross-sectoral and activities-based approach is taken with respect to regulation, this approach needs to be complemented by international coordination and mutual feedback, helping to ensure fair international competition and consistent regulatory approaches. This is especially important for American firms operating abroad, in jurisdictions that may apply different data protection and data security standards.

If new entrants (whether 'BigTech' firms or others) can offer comparable financial services from outside of the regulatory perimeter, using their platforms to reach large customer bases, then there exists a risk that they could reach a position of systemic importance without being subject to the same safeguards that have been applied to regulated institutions. Were such a new firm to reach a position of dominance in the provision of a particular service or transacting and holding funds for a significant cohort of the economy, this could ultimately threaten the gains in financial stability that have been achieved post-crisis.

Recommendation: Regulatory and supervisory frameworks should adhere to the fundamental principle of "same activity, same risk, same rules, same supervision." This principle should be promoted holistically, including on cross sectorial and cross border bases.

2. Regulatory cohesion, especially for cyber-security, is critical.

Notably, regulations affecting players in financial services extend beyond those issued by the financial agencies – with other regulations governing topical areas such as data protection and cyber resilience. A greater consistency or interaction between financial and non-financial regulations would help promote efficiency, in addition to promoting a competitive environment for all participants.

This is particularly pertinent in the case of **cyber-security**. The highly dynamic nature of the threat makes it critical that cyber-security regulation is efficient, such that firms can readily adjust their responses to the threats posed in an agile manner to protect their customers, companies, and investors, rather than be mired in unnecessary or duplicative regulatory reporting and compliance.

There are currently many different state and federal laws covering the same cyber-security topics, creating unnecessary duplication and overhead. For example, all fifty states now have their own breach notification rules, adding a substantial compliance burdens for firms, and a potential distraction from activities to improve resilience.

As recognized in Treasury's 1st Report, better coordination on cyber-security regulation is needed to enhance the resiliency of the sector. We support Treasury's recommendations for financial regulatory agencies to harmonize regulations, adopt a common lexicon, and harmonize interpretations and implementation of specific rules and guidance around cyber-security, and we encourage similar efforts on a cross-border basis.

Not only for cyber-security, an agile coordination among the different agencies Is necessary across the FinTech space. Several other jurisdictions are more readily able to embrace innovation, where they are supported by more streamlined regulatory structures.

Recommendation: Enhanced coordination between agencies and across different domestic and international jurisdictional levels should be a priority, both in terms of US federal and state agencies, and internationally. This is especially important in activities such as cyber-security breach reporting, where the introduction of a one-stop-shop mechanism for incident reporting would be invaluable, and the adoption of new innovations and products within the financial sector.

3. Data quality, integrity, and protection are cornerstones of the new digital economy.

Data is an area of great opportunity for better information and knowledge, has often been a catalyst for constructive new investments and innovations, and by itself is a valuable resource that warrants critical protection. **Data-driven innovations** will be at the heart of the digital transformation for all industries. For the data economy to become a reality, the first condition is to ensure the right incentives to generate high quality data, and to reward proprietary investment and innovation. All market participants should be encouraged to invest in systems, models, and teams that produce and utilize high-quality data, which in turn enable them to provide customer products and services more economically.

Where some other jurisdictions started to require banks to share data with new entrants, any such approach should be reciprocal and applied equally across sectors and to all players performing similar activities, including 'BigTech' firms. By the very nature of their business models, such firms often have a significantly higher degree of personal information, upon which to build their products and services.

While data sharing is at the heart of the open banking concept, and this may help to provide customers with more personalized products and services, there are several additional considerations in how such data is shared and used. **Protection of customers' data** should be a top priority, with a framework defined to ensure that all the players in the ecosystem put in place the necessary measures to comply with this. While customers are generally aware of the personal information that their bank or insurer holds, it is apparent that users of services from 'Big Tech' firms do not always have this insight.

Creating a FinTech ecosystem in which the sharing of data is secure (in all bonds of the chain), and where there is a certainty on who owns and how data is been stored and used, should be a

key priority. All companies wanting to provide financial services to a customer should be bound by the same rules and have the same high standard to ensure that the data is secure, for instance by extending the Gramm-Leach-Bliley Act requirements beyond just financial institutions, to the whole ecosystem. If this is ensured, then customers will be able to select, on a transparent and informed basis, from a range of trusted providers, underpinning a strong and uniformly regulated market in digital financial services.

In pursuing a common minimum level of security for all participants, we encourage Treasury to consider examples of efforts currently underway in other jurisdictions, such as Europe's General Data Protection Regulation (GDPR). Similarly, the Monetary Authority of Singapore (MAS) is developing a set of "Guidance on responsible use of data analytics" for all participants.[4]

The availability of increasing amounts of valuable data, including customer-specific information (acquired through telematics, sensors, wearables, etc) also requires a sound public policy discussion on responsible considerations on the use of that data, and the impact on the availability of financial products, such as affordable protection for higher risk (and potentially lower income) individuals.

Recommendation: Any potential initiatives for data access and sharing within the FinTech ecosystem should require (i) a consistent minimum level of data protection amongst all participants, and (ii) reciprocity amongst all participants.

4. **Incumbent firms must be able to adopt new technologies to compete and serve their customers.**

In this dynamic and evolving environment, it is important that incumbent firms are innovating, to keep pace with customer preferences and alternate offerings in the market. Where banks and insurers adopt new technologies, this is for the betterment of their customers through promoting customer choice, as well as enhancing firms' own risk management. As observed in the IIF-McKinsey 2017 report *The Future of Risk Management in the Digital Era*, digital innovations are increasingly being deployed within banks' risk functions, both to enhance risk management and gain improved insights, and in other cases to keep pace with the digitalization of the front-line, in support of customer fulfilment.[5] Similarly, insurers are constantly enhancing their abilities to identify, analyze and manage risk, including by applying new technologies (including customer-facing tools as well as tools for better risk and market data analytics).

Regulators and supervisors should encourage incumbent firms to pursue an agenda of increased digitalization to better meet the needs of their customers. Faced with such a dynamic competitive landscape, firms **must be able to adapt** and transform themselves to ensure their ongoing viability and profitability without fear of subsequent supervisory or enforcement actions, such as via No-Action Relief described by CFTC Chairman Christopher Giancarlo.[6]

Where the traditional paradigm of stability was a static one, there increasingly needs a more

[4] Monetary Authority of Singapore (MAS), *MAS and financial industry to develop guidance on responsible use of data analytics*, April 2, 2018, http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-and-financial-industry-to-develop-guidance-on-responsible-use-of-data-analytics.aspx

[5] IIF-McKinsey, *The Future of Risk Management in the Digital Era*, October 2017, iif.com/publication/regulatory-report/future-risk-management-digital-era

[6] Christopher Giancarlo, remarks at IIF Washington Policy Summit, April 19, 2018.

dynamic view – that **financial stability is about evolution and moving forward**, rather than standing still or looking backward. Restrictions on ability of incumbent institutions to transform themselves and adapt to the new environment might ultimately prove the largest threat to the system as a whole.

In this context, it is significant that banks and insurers move forward and innovate in a controlled and cautious manner, cautious in their experimentation and implementation of new solutions. Regulated financial institutions of all kinds recognize that their top asset is the trust they have with their customers, and, therefore, they maintain robust change management controls to ensure this trust isn't jeopardized.

The benefits of adopting new technologies at incumbent institutions outweigh the associated risks – for example, the Financial Stability Board has recognized that cloud computing can be safer, more robust, and better protected than legacy infrastructure.[7] Similarly, the IIF's recent study on machine learning in credit risk modeling and management highlighted that the adoption of these techniques is delivering greater accuracy in modeling, better use of existing data and additional insights from new data sources, and enhanced ability to overcome biases inherent in traditional modeling approaches.[8] Such initiatives are agents for transformation and data-driven decision-making, ultimately making banks and insurers stronger, more stable and secure.

Moreover, the regulatory structure should allow that **all participants can innovate under similar conditions**. It is critical that banks and insurers are provided a framework that allows them to onboard and develop innovative ideas, both in-house and through different methods of collaboration. Examples of asymmetries or barriers to banks and insurers innovating include:

- the banking prudential framework's requirements for consolidation of activities under a banking group, which places an extra layer of regulatory burden and lowers their capacity to innovate whether it's in-house, via acquisition or through a dedicated FinTech entity;
- legacy requirements on banks for third party management, which are designed to traditional vendors rather than FinTech innovators with whom banks might seek to partner; and
- accessibility of 'sandboxes'[9] for incumbent firms as well as new entrants, with the same level of flexibility.

Recommendation: Greater agility by regulatory agencies should be encouraged, along with collaboration with industry and other participants to develop the appropriate mechanisms (eg. sandboxes, hackathons, co-operation agreements) to enable safe and effective innovation, accessible equally to all participants, and subject to effective safe harbor protections. Third party management requirements should be reviewed for their applicability to FinTech innovators.

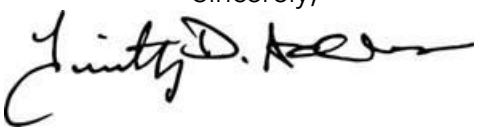
[7] Financial Stability Board, Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that merit authorities' attention, June 2017, http://www.fsb.org/2017/06/financial-stability-implications-from-fintech/

[8] IIF, *Machine Learning in Credit Risk*, March 2018: the IIF interviewed 58 banks and 2 mortgage insurers on their adoption and exploration of machine learning techniques in credit risk modeling and management.

[9] Regulatory "sandboxes" provide financial institutions and non-financial firms with a controlled space in which they can test innovative FinTech solutions with the support of an authority for a limited period of time, allowing them to validate and test their business model in a safe environment.

As always, the IIF stands ready to provide further input and any necessary expansions or clarifications on our comments. We look forward to our continuing engagement as the Treasury completes this 4th Report in accordance with the Executive Order. If you have any questions on the issues raised in this letter, please do not hesitate to contact me or Brad Carr, IIF's Senior Director of Digital Finance Regulation and Policy (bcarr@iif.com).

Sincerely,



Timothy D. Adams