International Banking Federation

5th Floor, One Angel Court
30 Throgmorton Street
London EC2R 7HJ
**tel**: + 44 (0)7725 350 259
**web:** www.ibfed.org

Secretariat of the Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 Basel
Switzerland
baselcommittee@bis.org

October 31, 2017

Dear Sir/Madam:

**Re: Implications of Fintech Developments for Banks and Bank Supervisors**

The International Banking Federation (IBFed[1]) appreciates the opportunity to comment on the consultative document issued by the Basel Committee on Banking Supervision (BCBS) in August 2017: "*Sound Practices: Implications of fintech developments for banks and bank supervisors*" (the **Consultative Document**).

The IBFed acknowledges that the Consultative Document provides a concise, high-level summary of both the current landscape of technical innovation within the financial services sector, and many of the key important challenges to the business models of banking institutions and non-bank technology companies. The Consultative Document's observations will be useful to banking industry participants, national supervisors and other parties interested in the policy implications of the rapid technological changes affecting financial services. It also underscores the important role that innovation and technological change have always played and continue to play in successful banking.

The IBFed would like to thank the BCBS for hosting an industry outreach event in New York City on October 17, 2017. The discussion was informative and ideas were actively

[1] The International Banking Federation (IBFed) was formed in 2004 to represent the combined views of our national banking associations. The IBFed collectively represents more than 18,000 banks, including more than two thirds of the largest 1,000 banks in the world. IBFed member banks play a crucial role in supporting and promoting economic growth by managing worldwide assets of over 75 trillion Euros, by extending consumer and business credit of over 40 trillion Euros across the globe, and by collectively employing over 6 million people. The IBFed represents every major financial centre and its members' activities take place globally. With its worldwide reach the IBFed is a key representative of the global banking industry, actively exchanging with international standard setters and global supervisory bodies on subjects with an international dimension or with an important impact on its members.

shared by all the participants. In addition to the importance to ensure a level playing field among all players regardless of the kind of legal entity, one of the key take-aways from the meeting was that banking agencies around the world are responsible for the oversight of banks and could not have the authority to provide direct oversight to fintech entities. Any international framework would be considered as doing little to bring non-bank fintech providers under consistent regulation. Today, some banking agencies start regulating how their banks interact with fintech companies. The October 17, 2017 meeting also highlighted how banks are benefitting from leveraging new technologies. And while there was general consensus that all entities providing bank-like services should be subject to the same level of oversight, it is also important not to smother innovation that could benefit consumers, banks and economies globally.

The IBFed wishes to highlight three fundamental points that must inform these policy discussions:

- The business of banking has always included a careful focus on the opportunities and attendant risks of technological change
- Financial technology continues to evolve quickly and its breadth and impact on jurisdictions is vast
- A properly balanced approach is required for creating a regulatory and supervisory fintech environment in which both newcomers as well as established businesses can flourish. Governments considering proposals related to fintech should ensure that the policy underlying the existing bank regulatory framework is maintained and that applicable rules are applied evenly and fairly across every entity that provides a financial service, whether it is a chartered financial institution or not. Regulators should be guided by a 'same-services/activities, same risks, same rules' principle. This would ensure high standards for consumer protection, market integrity and financial stability in a level playing field that supports fair competition and innovation. This is especially true when regulatory gaps can lead not just to competition issues but to safety risks for our society, such as in the case of AML/CTF rules.

**Innovation, technological change and related risks are fundamental to banking**

Technology plays a key role powering innovation in banking. Banks have always leveraged new technologies to deliver banking products in more effective ways, and that process continues today. The ultimate objective of innovation is meeting constantly evolving customer needs for financial services. Banks, in order to be successful, have always faced, and met this challenge.

Today's technologies are powering innovations that stand to deliver tremendous value to customers. Most fintech activities leverage technology to deliver, what is at its core, a fundamental banking service like lending or making a payment. The term "fintech" – often used to describe the convergence of technology and financial services – is now the moniker used for technology-focused start-up companies, but new methods of customer interaction, data analysis, transaction processing and other traditional banking functions must not obscure the underlying reality that this process is inherent in banking. Many of these activities are already captured by existing regulation. Appropriately, most regulators around the world have focused on regulating the banking activity being offered, not the technology that is being used to deliver it.

As noted in the Consultative Document, technological change may not only result in new risks, but also can open up new opportunities for banks and their customers[2]. Regulators should be focused on supporting this innovation while managing any new risks.

Collaboration among regulators will be essential to an effective regulatory framework, which both supports these opportunities and fosters management of the related risks that will be enhanced. If done correctly, it will serve to spread knowledge quickly, minimize inconsistencies, avoid conflicting guidance, and ultimately speed adoption of valuable innovations. As an example, one promising mechanism could be pilot programs, which can be important elements in technology deployment in a safe and sound manner. Pilot programs seem a natural area in which collaboration among regulators, at least for exchange of knowledge and information, will be important and speed adoption of beneficial technological innovation more broadly.

Banks and national supervisors are focused on both opportunities and risks of technological evolution. The Consultative Document notes risks on which banks and their national supervisors should focus as they implement technological changes. Among others are:

- Strategic, operational, cyber and compliance risk **(Observations 2 and 3)**
- Risks inherent in the use of third parties to outsource operations in pursuit of cost reductions, operational flexibility and other business objectives **(Observation 4).**

In many markets and national regulatory regimes, there are well-developed, detailed measures in place and active in response to these risks. For example, in the United States, the Federal Office of the Comptroller of the Currency **(OCC)**, which regulates nationally chartered banks, has put in place standards for regulating information technology risk[3], and other US regulators have adopted similar guidance. Similarly, the OCC established standards for risk governance, including operational and compliance risk, for large, complex banking institutions.[4] US regulators have also addressed specific concerns related to third-party service providers in such publications as the Information Technology Examination Handbook, published by the US Federal Financial Institutions Examination Council **(FFIEC)**, an umbrella group coordinating supervisory policies among US banking regulators.

EU regulators have similar standards for regulating technology risks.[5] EU legislators have defined standards for handling operational risks in the Capital Requirements Regulation as well as in the Capital Requirements Directive, which has to be implemented into national law at member states level.[6] National supervisors can issue further additional guidance. For example, in Germany the national supervisor published further guidance on risk

---

2 *See* Consultative Document, Observation 1.

3 Title 12, Code of Federal Regulations, Part 30, Appendix B. The U.S. Code of Federal Regulations is cited throughout as "CFR."

4 12 CFR, Part 30, Appendix D.

5 EBA Guidelines on information and communication technology (ICT) Risk Assessment Under Supervisory Review and Evaluation Process (SREP)

6 Part Three Title 3 of the Capital Requirements Regulation; EBA Guidelines on the management of operational risk in market-related activities; EBA Regulatory Technical Standards (RTS) on the conditions for assessing the materiality of extensions and changes of internal approaches for credit, market and operational risk

management (MaRisk)[7] which covers both operational risk as well as third-party risk. Additional guidance exists for annual auditors (Prüfberichtsverordnung), with a focus on operational risks and outsourcing. In Italy, the Central Bank defined a regulation on internal controls[8], which provides extensive measures on information governance, ICT risks and outsourcing risks. These activities are also analysed and supported with cooperative initiatives in the banking sector.[9] The European Banking Authority has also voiced its expectations in the SREP Guidelines.[10] The Committee of European Banking Supervisors (CEBS) issued guidelines on outsourcing in 2006. These guidelines are complemented by the EBAs current work on a recommendation on outsourcing to cloud service providers.[11]

Specific to changes in the retail payments marketplace, Canada's Department of Finance is examining a new risk-based oversight framework, balancing prudential needs with the interest to foster innovation and competition. Its intent is to create rules, based on the activities performed by a payment service provider (PSP), proportionally measured against the Government's policy objectives of safety and soundness, efficiency and consideration of users' interests.

Though these and other standards must continually evolve based on experience and input from the banking industry and the public, they make clear that national authorities and banking institutions are well aware of, and acting to, address the sorts of risks described in the Consultative Document.

One thing technology has fundamentally changed is the ability of technology driven companies to quickly reach customers and directly offer financial services. Today, a company does not need a branch network to reach a mass market. In many cases, this has allowed non-banks to develop direct customer relationships. While innovation at banks is closely watched by regulators, non-banks offering these services are not consistently captured as most regulators do not have jurisdiction to regulate non-banks. Jurisdictions should amend laws to ensure that banking regulators are able to monitor these companies to ensure that they are regulated consistently. This will ensure that customers are equally protected wherever they receive their financial services.

**The financial technology market continues to evolve quickly and is developing differently across the world**

Regulators around the world are carefully monitoring its development and taking action where necessary. Due to the rapid pace of innovation, regulators need flexibility to monitor

---

7 BaFin Mindestanforderungen an das Risikomanagement (MaRisk) - Minimum Requirements for Risk Management

8 Circolare 285 under Banking Supervisory Provisions.

9 ABI Lab Consortium, the Italian Research and Innovation Center promoted by ABI, monitors the evolution of technology in a cooperative manner with Italian banks, with regard of the regulatory and market impacts and promoting the growth of ICT skills in the banking community.

10 EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)

11 CEBS Guidelines on Outsourcing; EBA/CP/2017/06 Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010

developments in their market and respond quickly when needed. Premature regulation may impede innovation and risks failing to accurately capture appropriate activities as the market evolves. At the same time, technology has allowed financial service firms to quickly reach customers with new products. When abuses arise, regulators must move quickly to address them. Usually this means evaluating how a technology company's activities fit into existing banking regulatory frameworks. If pushing for any international framework should be premature at this stage it is also important to express support for comparably equivalent national regulatory approaches. The business models being developed and the risks associated with them are quite different in each country and the regulation needed in one market might not be appropriate for another. As such an international regulatory framework for fintech is not appropriate at this time. Marketplace lending, for example, looks very different in the U.K., where it is often peer-to-peer, than it does in the U.S., where institutional investors make up much of the funding. A one-size-fits-all approach to regulation would inevitably fail to address key risks in some areas and restrict innovation in others. This is why local regulators need the flexibility to tailor regulations to address the risks that develop in their markets.

The other consideration is that national regulators today are focused on bank entities and rarely encompass fintech players for whom this consultation document highlights. Therefore, an international framework that does not include oversight of fintechs will not address the evolving risks that have been identified requiring supervision.

**There are key areas where international coordination is needed and in many cases, is already underway**

Though most of the implications of technological innovation in financial services are best addressed through dialogue in national markets among banking institutions, their national regulators and the public, IBFed notes three areas in which cooperation across multiple geographic markets can be particularly important: maintenance and enhancement of cybersecurity, combating money laundering and terrorism financing with the aim to prevent risks for our society, and maintaining the strength and security of the international payments system. Existing regimes provide robust responses to address these risks.

In promoting cybersecurity, government authorities and private-sector financial institutions have participated since 1999 in the Financial Services Information Sharing and Analysis Centre (**FS-ISAC**). Initially focused on sharing information among US-centred governmental units and financial services firms, FS-ISAC from 2013 has grown to over 7,000 members in 37 other countries, actively working with government entities in those countries, as well as regional computer emergency readiness teams and industry associations. The FS-ISAC regime provides a significantly enhanced degree of coordination between public- and private-sector entities both to permit responses to specific threats and to share information acquired in the process that can support continuing enhancements in cybersecurity and resiliency.

In the European Union, several CERTs are established at national level, such as for instance, the Financial CERT that was established in Italy as a banking competence centre on cybersecurity issues involving the Italian Banking Association, the Bank of Italy and the banks. The CERT promotes info sharing, co-ordination in case of cyber emergencies and deepening of the best technological security solutions. Similar initiatives are being

implemented in the Scandinavian countries with the Nordic Financial CERT. These initiatives are strengthening the information exchange network with national law enforcement agencies and with Europol, and are giving valuable results in terms of response to computer attacks.

In combatting money laundering and terrorist financing, the Financial Action Task Force (**FATF**) is an inter-governmental body established in 1989 that now includes 35 member jurisdictions. The FATF sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering and terrorist financing within the international financial system. The FATF's recommendations and standards promote a coordinated response to these threats to the integrity of the financial system and the sharing of concepts and operational insights among members. The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. It also collaborates and shares information with other international stakeholders.

The U.S., Canada and numerous other jurisdictions have identified improving the speed, safety, and efficiency of cross-border payments as a priority. While each country or jurisdiction should be free to develop the best domestic payment system they can, it is important that international payments also be considered. With these cross-border payments comes required coordinated oversight from the regulators of each jurisdiction. As these payments approach real-time in speed of clearance and settlement, coordinated regulatory approaches become more important.[12]

The IBFed believes that these examples conclusively demonstrate that, in the three areas of cybersecurity, money laundering/terrorist financing and payments system protection, international coordination and cooperation is healthy and proceeding effectively through existing channels and cooperative efforts.

In addition, the IBFed has identified three other areas of concern that warrant additional review and international coordination by bank supervisors. Fintech activity in these areas presents new risks that supervisors should be prepared to mitigate.

The first is the credit risk posed by fintech crowd lending businesses. These lightly regulated firms should be subject to the same lending oversight as financial institutions to provide protection to consumers and investors.

The second is liquidity risk associated with high-frequency trading conducted by non-bank fintech companies. These unregulated or under-regulated parties may disrupt trading activities with multiple high-speed transactions in an effort to gain an unfair market advantage. This poses a threat to investors and conventional firms that are subject to regulatory oversight.

The third area of focus is the issue of accountability and liability in case of problems when

---

[12] *See Federal Reserve: Next Steps in the Payments Improvement Journey*, at https://www.federalreserve.gov/newsevents/pressreleases/files/other20170906a1.pdf (September 6, 2017), noting a number of standards-setting committees and similar organizations active in payments system policy matters in which the Federal Reserve participates.

banks and fintechs are both serving a shared customer. This risk may become more apparent as the Payment Services Directive 2 (PSD2) is implemented and fintech firms gain access to customer accounts to facilitate payments on behalf of the customer. The entire industry would benefit if comparable standards rules apply to fintechs and banks that are responsible for the moving customer funds.

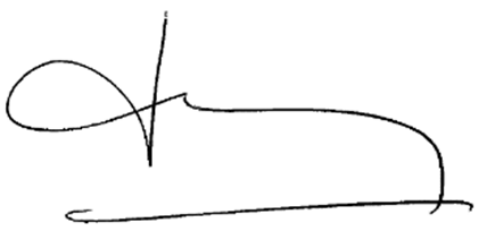
Regarding the potential contagion risk (step in risk) related to fintech we refer to the letter that was send to the Basel Committee on the 15th of May 2017.

## Conclusion

The IBFed appreciates the opportunity to provide comments on the Consultative Document. At this time, we support each jurisdiction's own bank supervisory agencies in their efforts to address the challenges and opportunities related to emerging fintech technologies while continuing to encourage comparably equivalent national regulatory approaches. Bank supervisors have the authority to supervise banks. Developing an international fintech regulatory framework may have its merits in certain circumstances, as is demonstrated by FATF for example, but could be premature regarding the fast-changing digital environment and because most bank supervisors don't have the authority to provide this oversight within their own jurisdiction let alone across borders.

We hope you find our comments on the Consultative Document useful. Please let us know if you have any further questions or would like to discuss our recommendations in further detail.

Yours sincerely,



Ms. Hedwige Nuyens
Managing Director of the IBFed

Mr. Stephen K. Kenneally
Chair of the IBFed Value Network Transfer Working Group

Ms. Debbie Crossman

Chair of the IBFed Prudential Supervision Working Group