FBF RESPONSE TO BCBS CONSULTATION
CONSULTATIVE DOCUMENT – SOUND PRACTICES: IMPLICATIONS OF FINTECH DEVELOPMENTS FOR BANKS AND BANK SUPERVISORS

Publication Date: August, 2017

Deadline: October 31 2017

Author: French Banking Federation (FBF)

N°	Recommendation	FBF's answer	Comments
INTRODUCTION			
		The French Banking Federation (FBF) particularly welcomes this opportunity to comment the BCBS' observations and recommendations regarding the implications of the Fintech developments for Banks. Please note that FBF will only provide comments on the first four recommendations. Firstly and as a reminder, FBF would like to underline that its **definition of the FinTech is aligned with the one given by the FSB stating** that it should be understood as "finance enabled or provided by via new technologies meaning the application of new technologies to financial services". As technology-enabled innovation in financial services does not depend on the size or legacy of a firm and as innovative financial technology-based solutions and services are being developed by Banks, we find particularly accurate for risk assessment purposes the definition by the BCBS of **3 categories of players: Incumbent Banks, FinTech start-ups and Big Tech firms** (including GAFA, BATX, Telcos, Transportations, Utilities, IoT services…).	

A. OPPORTUNITIES			
1	**<u>Observation 1</u>: The nature and the scope of banking risks as traditionally understood may significantly change over time with the growing adoption of fintech, in the form of both new technologies and business models. While these changes may result in new risks, they can also open up new opportunities for consumers, Banks, the banking system and bank supervisors.** **<u>Recommendation 1</u>: Banks and bank supervisors should consider how they balance ensuring safety and soundness of the banking system with minimizing the risk of inadvertently inhibiting beneficial innovation in the financial sector. Such a balanced approach would promote the safety and soundness of Banks, financial stability, consumer protection and compliance applicable laws and regulations, including anti-money laundering and countering financing of terrorism (AML/CFT) regulations, without unnecessarily hampering beneficial innovations in financial services, including those aimed at financial inclusion.**	**Firstly, it seems necessary to underline that the Banks are FinTech companies too.** The banking industry is often the source of the innovation in the financial sector. This innovation is built by the knowledge of the need of theirs clients and the joint work carried out with FinTech start-ups. It is worth pointing out that **Banks do a lot of FinTech themselves**, in the meaning of developing innovative, technology-based financial solutions and services. This comes with **huge investments**, jobs and growth, for all sorts of suppliers (including incumbent tech giants). While there are still strategic reasons for Banks to **rely on internal IT departments**, there is considerable potential to create value — for themselves and the economy at large — by **nurturing an ecosystem of start-ups and technology innovators** that can assist Banks in developing shared platforms, increasing resilience and cost effectiveness of banking and payment systems. Moreover, several Banks have set up some physical infrastructures to offer a framework for giving good conditions to nurture the start-ups and elaborate a **partnership with FinTech small firms.** One of the challenges is that smaller companies are often less ready to meet all the regulatory requirements that Banks need to adhere to so there is often support from Banks' compliance areas to bridge the knowledge gap. **<u>Customer protection</u>:** **With regard to customer protection**, existing regulations provide a solid level of protection and will continue to do so. A prerequisite is to ensure that consumers are protected and that the financial stability is ensured, irrespective of who the provider is. Therefore, it is necessary to maintain **a level playing field** regarding the regulation of potential competitors/sectors and between Members States. Current asymmetries hinder innovation, for example for traditional banking players subject to the existing banking financial regulation. They can also create **risk situations for consumers** who do not have a homogeneous level of protection but also for all the financial institutions. For example, financial institutions can be directly affected by fraud problems linked to	

		cyber security issues encountered by certain actors, or more indirectly by the weakening of the consumer confidence in financial services. **The same regulatory conditions and supervision should apply to all actors who seek to innovate and compete on Fintech**: **Incumbent Banks, FinTech start-ups and Big Tech firms.** The authorities must always apply the "same services/activities, same risks, same rules, same supervision" principle in order to ensure consumer protection and market integrity. As the value chain includes different kind of actors and becomes more complex, all firms should go through the same process from product design to sales to avoid any regulatory arbitrage in responsibility-sharing. In a more detailed view, consumer protection will rely on: - **Cross-border operations:** Maximum harmonisation of consumer-protection rules in retail financial services has not prevented divergence in national legislations, particularly due to EU Member States' growing tendency to gold-plate, either when transposing or in the extensive interpretations of the texts by national regulators. Additionally, there is a need to extend the regulation in place to non-regulated FinTech firms in order to address cross-border issues. - **Solvency:** In the area of credit granting, the principles of solvency analysis are governed by the Mortgage Credit (MCD) and Consumer Credit (CCD) Directives. It is important to ensure that they are respected, including by new actors, notably those who operate remotely and bring innovative models. It will help ensure that the consumer is protected, with a focus on the **risk of over-indebtedness.** However, some texts cover only credit institutions. Some specialized or alternative actors, who have pushed for the creation of new accreditation categories in certain countries and for crowd-lending, are not always subjected to the same requirements and supervised in the same way, which creates a distortion and does not guarantee good consumer protection. - **Information disclosure:** customer information is subject to many obligations for all financial services. EU measures such as the MCD, the CCD, the PAD, the Undertakings for Collective Investment in Transferrable Securities (UCITS) Directive, MiFID II, PRIIPss Regulation and IDD insure that information disclosure	

is effective, transparent and comparable. We think that no new regulation is required at the moment, and that it is preferable to make use of existing extensive regulation protecting consumers and give them time to produce their effects and to assess if they apply to all players. However, the consumer protection legislation has not always been thought of for the digital environment. An evaluation of the impact of all existing regulatory texts to remote operation modes via mobile or internet should be carried out. In our view, any new requirement on additional information to provide to the consumer should be considered with caution. The priority should be to adjust the already adopted measures to the new digital technologies, and to respect the principle of proportionality. It means not creating inflexible and excessively detailed rules that prevent the Banks from developing their products and services in line with new technologies, which has the effect of distorting competition with less regulated players.

- **Complaints handling procedures:** Unfair, deceptive or aggressive commercial practices and unfair terms are already largely regulated. As far as regulated Fintech Banks are concerned, the consumer protection is fulfilled thanks to several directives such as the Consumer ARD Directive or the Financial Dispute Resolution Network (FIN-NET) founded in 2001 for cross-border operations, which could be expanded. In the meantime, an issue to look into in the context of consumer protection is the legal liability of each actor involved in a given service. As such, it could be argued that the best approach for ensuring consumer protection is for Banks to take a risk-based approach to mitigating and controlling for possible consumer protection risks.
- **Data protection:** The GDPR is a major step forward. Any additional regulations on this subject would be counterproductive at this stage.
- **Financial inclusion:** The adoption by customers of new digital services requires that these technologies be explained, popularized and validated by an undisputed body. The risk of financial exclusion linked to a low level of financial education is real and effectively reinforced by the use of digital. It mainly concerns people who are financially fragile, disabled or elderly. The integration of these people will mainly be through digital and financial education to be integrated into school curricula, global public policies, and programs developed by Banks to support digital awareness and security. As the PAD is currently being transposed, a

		European regulation on this point does not appear necessary. In any event, any initiatives that might be taken should involve all actors, including those who do not currently have obligations to serve non-digital consumers. **AML/CFT/KYC obligations:** **With regard to AML/CFT purposes**, it may be appropriate to explore the different national approaches. Not all FinTech firms have been designated as "obliged entities" in all EU Member States, even where they provide similar services to firms that have been designated as such. The new financial players may also be outside the scope of the banking sector regulation and subject to less stringent AML/CFT rules that are Banks. These regulatory gaps or loopholes may lead to some distortion of competition, which may violate the level playing field principle and lead to increased potential for financial crimes. **Regarding customer identification and verification remotely and through digital means**, the differences in the ways in which the Directive 2005/60/EC was transposed by Member States have a several consequences. They could hamper the development of FinTech firms using innovative CDD solutions. They also represent a big obstacle to a harmonized European digital identity framework as eIDAS could be. We are in favour of providing for **a broad scope of possible methods to be used in the process of digital on boarding**, ranging from those notified in line with the eIDAS Regulation to others. As different national requirements still apply to remote identification of customers, harmonization is required, as a first step, notably to allow digital on boarding including via video. The **financial industry compliance obligations** (i.e. KYC, AML, etc.) could be more efficient if there were a regulatory framework that allowed public/private institutions to provide services related to KYC. In conclusion, it is necessary to **harmonize the European framework regarding the prevention of money laundering and terrorism financing (AML/CFT), to ensure that the 4th Anti-Money Laundering directive is implemented in a consistent way as the acceptance of the means for identifying customers remains on the Member States.**	

<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">B. KEY RISKS</td><td></td></tr>
<tr><td>2</td><td><u>Observation 2</u>: For Banks, the key risks associated with the emergence of fintech include strategic risk, operational risk, cyber-risk and compliance risk. These risks were identified for both incumbent Banks and new fintech entrants into the financial industry.

<u>Recommendation 2</u>: Banks should ensure that they have effective governance structures and risk management processes in order to identify, manage and monitor risks associated with the use of enabling technologies and the emergence of new business models and entrants into the banking system brought about by fintech developments. These structures and processes should include:
- robust strategic and business planning processes that allow Banks to adapt revenue and profitability plans in view of the potential impact of new technologies and market entrants;
- sound new product approval and change management processes to appropriately address changes not only in technology, but also in business processes;
- implementation of the Basel Committee’s Principles for sound management of operational risk (PSMOR) with due consideration to fintech developments; and</td><td>We recognize that the key risks associated with the emergence of FinTech, and the increasing number of interactions/partnerships between Banks and Fintech startups, are: strategic risk, operational risk, cyber-risk and compliance risk. Nevertheless, we would like to highlight the following concerns about other risks relative to the development of FinTech:

- Credit risk: The crowd-lending business carry a credit risk and some bankruptcy examples reminded this reality for consumers and investors, during the last few months. The financial intermediaries in crowd-lending should be submitted to the same requirements as the leading players which risk is supervised. Indeed, it is essential to modify the regulation to prevent any financial risk.

- Liquidity risk: The development of the high-frequency trading (HFT) by some FinTech firms requires to strengthen the liquidity regulation. This activity modifies the organization of equity markets, as well as the organization of trading platforms. When they provide liquidity to capital market without regulatory requirement, FinTech firms specialized in HFT evict traditional actors with a distortion of the competitive environment. These new unregulated actors could generate sudden « flash crash » through market manipulations strategies (they send a disproportionate number of orders dedicated not to be executed with the aim to slow the functioning of trading platforms and to benefit from trading opportunities) and benefit from the lack of the current regulatory framework.

- Step-in risk: Any operational adverse event could impact the reputation of small and big stakeholders and damage the financial environment, by contagion. As such, the operational risk could oblige FinTech partners/owners to intervene (step in risk) due to the absence of capital or recovery requirements.

- Recovery and resolution risks: Interactions between FinTech start-ups and credit institutions are increasing. Even if the development of FinTech allows an</td><td></td></tr>
</table>

	- monitoring and reviewing of compliance with applicable regulatory requirements, including those related to consumer protection, data protection and AML/CFT when introducing new products, services or channels.	improvement of reporting and monitoring processes, thus facilitating operational continuity in resolution period; the increasing digitalisation of the financial ecosystem may also speed up the movement of deposits in a time of crisis and could modify the timing of the determination when an institution is « failing or likely to fail ». The key question considered during such a failing situation is: which actor manages the customer relationship or interface, and which actor ultimately provides the services and takes the risk? At this time, it is not clear how resolution authorities can apply their resolution powers to those FinTech entities. It seems essential that a proper set of rules apply to fintech firms entering in the financial markets in order not to create further undesirable impediment to recovery/resolution for Banks or unnecessary external impediment to resolution for Resolution Authorities. - **No sand-box:** We support the implementation of a fair and harmonized regulatory framework for credit institutions and FinTech start-ups and we are not supportive to a "sandboxing regime" that would be circumscribed to a limited number of start-ups rather than applicable to all entities/activities including within a banking group. Besides, the significant number of sandboxing regimes, innovation hubs or similar regimes vary between countries. The Basel Committee should assess the various regimes of sandboxes in order to harmonize supervisory practices. Moreover, no soft or specific regulatory framework should be implemented to a specific actor. Requirements should apply to all the FinTech actors (new entrants FinTech and Credit Institutions). For this reason, we do not support the introduction of protective measures. Any regime introducing regulatory distortions would be dangerous and contrary to the financial stability and to the consumer protection. Rules should be the same for all stakeholders, small or big, new entrant or established actors.	

C. IMPLICATIONS OF USING INNOVATIVE TECHNOLOGIES	

3	**<u>Observation 3</u>: Banks, service providers and fintech firms are increasingly adopting and leveraging advanced technologies to deliver financial products and services. These enabling technologies, such as artificial intelligence (AI)/machine learning (ML)/advanced data analytics, distributed ledger technology (DLT), cloud computing and application programming interfaces (APIs), present opportunities, but also pose their own inherent risks.** **<u>Recommendation 3</u>: Banks should ensure that they have effective IT and other risk management processes to address the risks of new technologies and implement the effective control environments needed to properly support key innovations.**	Firstly, it is important to mention that technology has been implemented in Banks for decades, and efficiency improvement was always a driver in four major segments: - Interaction and communication with clients (from paper to online); - Security of the data and funds protection for their clients; - Enhancement of interoperability by way of standardisation and common rules (e.g. SEPA); - Industrialisation and automation in operations. A high percentage of Banks views the possibility of **partnerships with FinTech start-ups, or other actors of the FinTech,** with great interest. The objective is to obtain concrete benefits that enhance specific key business areas, products and/or services by leveraging: - Solutions that focus on cost reduction via process improvement or replacement of platforms/ IT solutions by either new business models or technologies; - Solutions enabling Banks to attract and on-board new customers, to improve customers' relationship or to increase the offer of new and innovative products/services; - Risk management; - Cybersecurity (e.g. fraud detection and data protection); - Regulatory (RegTech); - Big data and artificial intelligence; - Current processing solutions in the payments or securities space. The arrival of FinTech start-ups has spurred innovation, accelerated the transformation of Banks and opened door to new win-win collaboration. As an example, the FinTech could bring solutions in the payments or securities field: - **Distributed Ledgers Technology (DLT):** was initially popularized through the exchange of the digital currency Bitcoin. However, DLT may have many potential applications beyond digital currencies, many of which are relevant to the financial services industry. Distributed ledgers can provide for the development of more efficient trading platforms and payments systems, as well as providing more	

			transparent information sharing between financial institutions and between financial institutions and regulators. Properly developed, it can lead to a win-win situation for financial institutions and regulators, allowing firms to reduce operational costs and providing regulators with greater transparency and risk reduction in the financial system (e.g. via the development of a proper business case at Banks and industry level). DLT is the innovation where collaboration with other market players will be most needed as no DLT system will be possible without global and far-reaching collaboration. - **Interoperability** could be in relevant areas, provided it is developed in a way that ensures high levels of cybersecurity, data safety and customer protection, fair competition (the actors that use an infrastructure have to pay for its real cost). A wide adoption of Applications Programming Interfaces (APIs) will pave the way for a secure, competitive and innovative environment for financial services. The standards and interoperability must be defined at sector level and not supervision level. Various standards for many types of transactions and services have been defined in the banking sector over the years. Furthermore, the complexity of the standards makes the process of definition and sharing among the players complex, since it is necessary to take the operating and technological needs of all of them into account. Nevertheless, prescriptive regulations should be avoided. The European Commission should support the creation and/or adoption of proposed technical standards (on a voluntary basis) with a view to greater flexibility in the development of global technology solutions. From the point of view of security, guidance from supervisors on which standards to follow, such as NIST, ISO 2700X or COBIT would ease compliance. In addition, authorities can be helpful by delivering the Regulatory Technical Standards in advance to allow sufficient time for the industry to adapt. - **Real time payment:** Today the financial industry relies on a network of correspondent Banks that allow payments to be made cross-borders on average on a T+1 / T+2 basis (though this timescale can extend especially if there are compliance/legal rules to follow e.g. because of the country of the payee). A	

		number of Banks have been reviewing new blockchain-based payment protocols available on the market like Ripple and experimenting with a proof of concept platform based on Ethereum. These solutions take advantage of the capabilities of blockchain to execute payment obligations netting and enable real-time clearing without the involvement of correspondent Banks on each transaction.	
D. FOCUS ON OUTSOURCING AND PARTNERING RISKS			
4	**Observation 4: Banks are increasingly partnering with/and outsourcing operational support for technology-based financial service providers, including fintech firms, causing the delivery of financial services to become more modular and commoditised. While these partnerships can arise for multiple reasons, outsourcing typically occurs for reasons of cost-reduction, operational flexibility and/or increased security and operational resilience. While operations can be outsourced, the associated risks and liabilities for those operations and delivery of financial services will remain with the Banks.** **Recommendation 4: Banks should ensure they have appropriate processes for due diligence, risk management and ongoing monitoring of any operation outsourced to a third party, including fintech firms. Contracts should outline the responsibilities of each party, agreed service levels and audit rights. Banks should maintain controls for outsourced services to the**	With regards to security, financial actors are subject to a specific supervisory regime as a result of their activities, which is more supervised than other sectors. We believe it is necessary to **extend the scope of cybersecurity regulation and supervision to all players who offer financial services and manage financial data**. The security constraints imposed by regulators must be the same for all actors who handle or collect personal and bank data from end-to-end with the highest level of security (no weak link). At European level, the European Commission wants to promote competition and innovation among financial players by **"opening up" certain systems**. It is necessary that these initiatives **not be detrimental to the soundness (and even the "usability") of the systems in place.** Several points should be highlighted: - The FinTech firm, which intervene between the client and the Bank, should **not conceal the information necessary to detect the fraud**; - The **personal and banking information of Banks' customers must be protected against the leakage of information**, in the internal systems but also and especially in the "new actors" who consume this information and when they circulate between actors. This dissemination of information can facilitate **identity theft** or the development of models based on the **monetization of customer financial data**;	

	same standard as the operations conducted within the bank itself.	- The responsibility of each of the actors must be clearly defined in the event of an incident. Cybersecurity threats remain one of the most important challenges for Banks. As recently confirmed by Europol in the wake of the Wannacry ransomware attack, Banks have made substantial progress on this front compared to other sectors of the economy. More needs to be done and increased cooperation among the regulatory and supervisory authorities at national, European and global level will enhance progress on this front significantly. The EU could play a role in: - **Streamlining harmonised format and procedures for security (IT)** incident reporting to avoid overlap and redundancy in reporting to multiple competent authorities (NIS Directive, PSD2, Data protection regulation, Single Supervisory Mechanism SSM). - **For resilience purpose and risk mitigation**, establishing a legal framework for data sharing which allows the possibility to sensitive information related to fraud & cyber-attacks at national and cross-border level should be put in place. - **The current collaboration between the industry and regulators and among regulators needs improvement.** This would help to overcome the regulation challenges and maintain the speed of innovation/digitalization. The public sector needs to work proactively with the private sector, across borders, to share information about attacks, exchange best practices and continually improve security systems to deter cyber criminals. Harmonisation across jurisdictions could be prioritise through the fast adoption of guidelines to ensure **a common approach by regulators/supervisors regarding procedures and methodologies.** It is essential to update EBA Guidance on outsourcing, which dates back from 2006. It needs to be adapted to the cloud computing technology.	

		Nevertheless, these rules should cover an ecosystem that is increasingly trans-sectorial. Whether they are traditional Banks, or new entrants, all actors rely on GAFA today. Therefore, GAFA become new systemic institutions. A "prudential" supervision of these players should be studied.	