EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Position of the European Financial Congress[1] in relation to the Basel Committee on Banking Supervision's consultative document on Implications of fintech developments for banks and bank supervisors[2]

Methodology for preparing the answers

The answers were prepared in the following stages:

Stage 1

A group of experts from the Polish financial sector were invited to participate in the survey. They received selected extracts of the Basel Committee's consultative document translated into Polish and were asked to present their comments on the proposals put forward in the document. The experts were guaranteed anonymity.

Stage 2

The survey project coordinators from the European Financial Congress prepared a draft synthesis of opinions submitted by the experts. Responses were obtained from experts representing:

- banks,
- fintech companies,
- insurance companies,
- regulatory institutions,
- consulting and law firms,
- the academia.

The draft synthesis was sent to the experts participating in the survey with the request to mark the passages that should be modified in the final position and to propose modifications and additions as well as marking the passages they did not agree with.

Stage 3

On the basis of the responses received, the final version of the European Financial Congress' answers was prepared.

---

[1] European Financial Congress (EFC – www.efcongress.com). The purpose of the EFC is to promote debate on how to ensure the financial security and sustainable development of the European Union and Poland.

[2] https://www.bis.org/bcbs/publ/d415.pdf

Comments of the European Financial Congress
on the recommendations
put forward in the consultative document

1. Observation: *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.*

Recommendation 1: *Banks and bank supervisors should consider how they balance ensuring the safety and soundness of the banking system with minimising 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 with 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.*

It is essential to strike a balance between addressing the aspect of risk associated with advanced IT technologies in the financial sector on the one hand, and the implementation of innovative solutions which drive banking sector competitiveness on the other hand.

It is worth noting that fintech innovations are generated both by new players, i.e. fintech companies, and by banks, which are often quite innovative, depending on the market they operate in.

Ensuring system and client security should, however, remain paramount. Trust and security are two key development factors for the banking sector. It is worth emphasizing that banks are responsible for their clients' security, while regulators are in charge of the security of all entities engaged in relevant business activity.

2. Observation: *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.*

Recommendation 2: *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*
- *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.*

Banks should definitely ensure effective governance structures and risk management processes. However, it should be emphasized that these are universal recommendations and should apply to both banks and fintech companies. The scope of relevant management should first and foremost be correlated with the size of the target market and risk, rather than with the form of business activity (a bank vs. fintech company).

As regards operational activity, it is necessary to ensure effective compliance governance and the management of operational risk related e.g. to the collaboration between banks and fintech companies or to the direct implementation of fintech solutions in banks' operating processes. In the current market situation, it is also necessary to include fintech in strategic planning.

Fintech companies should be verified using due diligence procedures before they are engaged as partners and assessed through periodic audits thereafter. Banks should approve new products not only by considering customers' expectations as to their convenience (as is current practice), but also as regards security, including IT security.

3. Observation: *Banks, service providers and fintech firms are increasingly adopting and leveraging advanced technologies to deliver innovative 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.*

Recommendation 3: *Banks should ensure they have effective IT and other risk management processes that address the risks of the new technologies and implement the effective control environments needed to properly support key innovations.*

In a general sense, this recommendation is valid, but it seems not to be sufficiently specific. It might be useful to recommend best practices to be used by banks.

IT risk should be separated from operating risk and should be included in the risk management process of the entire bank or of a different entity, such as a fintech company. In the digital era, the management of IT risk should be prioritized higher and given suitable attention as early as the strategic planning stage.

Besides technical processes, it is also important to take into account educational activities addressed to clients concerning the safe use of banking products, e.g. the importance of the privacy of clients' authentication details.

4. Observation: *Banks are increasingly partnering with and/or outsourcing operational support for technology-based financial services to third-party service providers, including fintech firms, causing the delivery of financial services to become more modular and commoditised. While these partnerships can arise for a multitude of 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 the financial services 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 same standard as the operations conducted within the bank itself.*

In practice, banks have the appropriate guidelines and regulations in place to clearly define the scope of responsibilities and control for their collaborating partners.

The same criteria should be applied to fintech companies.

It is important to pinpoint the exact SLA parameters in agreements and to scrutinize partners (through due diligence and audits). In the case of outsourcing, it is impossible in practice to ensure the same degree of control for internal processes, and this is therefore replaced by partner evaluation and an appropriate agreement.

5. Observation: *Fintech developments are expected to raise issues that go beyond the scope of prudential supervision, as other public policy objectives may also be at stake, such as safeguarding data privacy, data and IT security, consumer protection, fostering competition and compliance with AML/CFT.*

Recommendation 5: *Bank supervisors should cooperate with other public authorities responsible for oversight of regulatory functions related to fintech, such as conduct authorities, data protection authorities, competition authorities and financial intelligence units, with the objective of, where appropriate, developing standards and regulatory oversight of the provision of banking services, whether or not the service is provided by a bank or fintech firms.*

It is essential not to differentiate between regulations and requirements depending on the legal status (a bank vs. a fintech company), as stated in the recommendation. The level of regulation should depend on the type of activity undertaken and on its scale, and thus on the associated risk. Activity of a strictly banking nature should be performed by banks (while it should be clear what type of activity is defined as banking activity); however, there obviously exist various types of activity of a banking nature, which may be undertaken by both banks and fintech companies.

Dialog with public entities, as well as with organizations which bring together financial institutions (e.g. banking associations) or payment/fintech organizations, is key to protecting consumers from threats. It may also enable the development of better standards and legal regulations. Apart from the dialogue with public entities, it is

important to address the issue of having fintech firms embrace the code of good practice in complaint process management.

An open industry dialogue and an exchange of experience should also have a positive impact on the level of education of banking sector employees, helping them to stay abreast of new directions and products.

6. Observation: *While many fintech firms and their products – in particular, businesses focused on lending and investing activities – are currently focused at the national or regional level, some fintech firms already operate in multiple jurisdictions, especially in the payments and cross-border remittance businesses. The potential for these firms to expand their cross-border operations is high, especially in the area of wholesale payments.*

Recommendation 6: *Given the current and potential global growth of fintech companies, international cooperation between supervisors is essential. Supervisors should coordinate supervisory activities for cross-border fintech operations, where appropriate.*

Cross-border payments are an important area for the development of cashless payments, as well as for enhancing access to financial services. At the same time, it is one of the areas most vulnerable to fraudulent transactions and money laundering (AML/CFT).

International cooperation between supervisory bodies is of key importance for preventing fraudulent transactions. National authorities should be involved in supervision of e.g. cross-border fintech companies.

It is also necessary to provide consumers with assistance and protection, where possible at the same level as is warranted when they use an entity based in their usual country of residence. This is especially important for online activities, as these are largely independent of territorial borders.

7. Observation: *Fintech has the potential to change traditional banking business models, structures and operations. As the delivery of financial services becomes increasingly technology-driven, reassessment of current supervision models in response to these changes could help bank supervisors adapt to fintech-related developments and ensure continued effective oversight and supervision of the banking system.*

Recommendation 7: *Bank supervisors should assess their current staffing and training models to ensure that the knowledge, skills and tools of their staff remain relevant and effective in supervising new technologies and innovative business models. Supervisors should also consider whether additional specialised skills are needed to complement existing expertise.*

No effective supervision may be ensured without an understanding of the mechanisms underlying the emerging fintech solutions. It is worth looking to developed markets for examples to follow. A valuable practice, used for example in English-speaking countries, is to exchange experience between regulators and the regulated entities by organizing

secondment schemes for employees. This may be an effective way to enhance the qualifications of regulators' employees.

Modern financial services are inextricably linked to new technologies and therefore it is essential for supervisory bodies to have the relevant expertise and necessary specialist skills in this area (to work with suitable experts). The level of knowledge possessed by the supervisor should correspond to that of the market – this is the only way to provide effective supervision.

8. Observation: *The same technologies that offer efficiencies and opportunities for fintech firms and banks, such as AI/ML/advanced data analytics, DLT, cloud computing and APIs, may also improve supervisory efficiency and effectiveness.*

Recommendation 8: *Supervisors should consider investigating and exploring the potential of new technologies to improve their methods and processes. Information on policies and practices should be shared among supervisors.*

Knowledge sharing among supervisory authorities is key. The implementation of advanced technologies will enable a reliable analysis of supervisory data, which will make it possible to increase the effectiveness and efficiency of supervisory activities, including better and earlier detection of violations, thus improving the security of clients and of the banking sector as a whole.

9. Observation: *Current bank regulatory, supervisory and licensing frameworks generally predate the technologies and new business models of fintech firms. This may create the risk of unintended regulatory gaps when new business models move critical banking activities outside regulated environments or, conversely, result in unintended barriers to entry for new business models and entrants.*

Recommendation 9: *Supervisors should review their current regulatory, supervisory and licensing frameworks in light of new and evolving risks arising from innovative products and business models. Within applicable statutory authorities and jurisdictions, supervisors should consider whether these frameworks are sufficiently proportionate and adaptive to appropriately balance ensuring safety and soundness and consumer protection expectations with mitigating the risk of inadvertently raising barriers to entry for new firms or new business models.*

It is vital to strike the right balance between the necessary level of caution and the indispensable openness to new solutions.

Supervision should cover entities not only due to their formal status (e.g. banks), but it should also apply to all entities, depending on the services they offer and the scale (e.g. fintech companies operating within or on the borderline of regulated activity).

It is also worth emphasizing the role of market participants as experts and advisors, to avoid being limited to regulators' in-house experts only.

The overriding aim of supervisory authorities is to ensure the security of consumers / clients (rather than the convenience of services) and hence supervision should extend to areas which may constitute a major risk, regardless of the legal status of the entities affected.

10. Observation: *The common aim of jurisdictions is to strike the right balance between safeguarding financial stability and consumer protection while leaving room for innovation. Some agencies have put in place approaches to improve interaction with innovative financial players and to facilitate innovative technologies and business models in financial services (eg innovation hubs, accelerators, regulatory sandboxes and other forms of interaction) with distinct differences.*

Recommendation 10: *Supervisors should learn from each other's approaches and practices, and consider whether it would be appropriate to implement similar approaches or practices*

Mutual exchange of experience and education facilitate the development and implementation of the best methods and practices.

11. Other comments

In summary, it is important to note that the recommendations are highly praised by experts participating in the EKF study, while the claims included in them are quite justified.

It is worth pointing out the following important and universal elements:

- It is necessary to educate all parties, including the supervisory bodies, suppliers and clients, so that secure operations can be warranted.
- It is recommended that supervisory bodies share their knowledge among themselves and cooperate with the market.
- The pursuit of convenience should not trump the importance of security, which is paramount in the financial sector and is the core reason for the existence of supervisory authorities.
- The level of supervision and regulation should be adequate to the operations and their scale, as well as to the associated systemic and client-related risks, rather than to business status only.