German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Response to the Basel Committee on Banking Supervision's consultative document on the implications of FinTech developments for banks and bank supervisors

Register of Interest Representatives
Identification number in the register: 52646912360-95

Contact:
Dr. Friedrich G. Zuther
Telephone: +49 30 2021-2100
Fax: +49 30 2021 192100
E-mail: F.Zuther@BVR.de

Berlin, 27 October 2017

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.
Collectively, they represent approximately 1,700 banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Fax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Comments

The German Banking Industry Committee (GBIC) welcomes the Basel Committee's initiative to examine the effects of FinTech for banks and banking supervision. From the perspective of German banks, the study is largely comprehensive and accurate, yet it urgently needs supplementing by a globally important aspect.

By definition, banking business comprises (i) risk transformation, (ii) maturity transformation, and (iii) scale transformation – none of these factors is directly changed by the rise of FinTechs. Risk is a fundamental element of a free-market economy – as long as decision-makers take responsibility for the (future) consequences of their actions. Any technological development forms part of the dynamic development of a free market, which is a normal situation. FinTechs stand for new technology, but this is independent from the size of the company – whether it is implemented by an existing bank or a start-up. In general, the principle of "same business, same risk, same regulation" should be the overall principle guiding every kind regulation (taking into account that any regulation is interference to a free market economy).
The main change brought about by digitalisation (and only to a limited degree by FinTechs) is the emergence of global internet juggernauts, both from the West (Google, Facebook, Amazon) and the East (Baidu, WeChat, Alibaba). Their business model of monetising customer data for advertising is a huge change to the industry in general – including banks. Therefore, European banks have to be aware of regulatory arbitrage as well as global arbitrage, both of which are outside the traditional scope of the BIS.

This is why **we see an urgent need to include an aspect that is missing from the recommendations, and to treat this with utmost priority**.

From our point of view, regulators not only have the duty of supervising individual players to ensure a fair and secure state of play whilst observing the rules – but in particular, to ascertain a level playing field and fair rules. In the wake of digitalisation, the game has already changed - to an extent that urgent action is required:

- according to the current EBA survey on FinTechs (which is currently in the process of consultation), 30% of FinTechs surveyed are unregulated;
- on page 29 (box #6), the discussion paper concerning AML/CFT states that new players are acting outside the existing regulatory regime, which distorts the competitive environment – whereby chapter 2 (on distributed ledger technology) does not even mention BitCoin.

In fact, these gaps in the system not only concern AML/CFT – they compromise the existing system as such. There is little point in regulators 'tightening the net', when there is a gaping hole in that net. These issues are not some distant future scenario: BitCoin is already big in the market, with successor technologies becoming established. This issue may be exacerbated abruptly once the 'BigTechs' – which the survey correctly portrays – enter the market. There is urgent need for action in this respect, which makes all the other aspects that the survey correctly identifies pale by comparison.

0) German banks therefore suggest giving priority to adapting the regulatory canon (above all calls for action mentioned in the survey) in order to ensure full coverage of the financial markets, and to create a level playing field, with the same rules applicable to all players. In this context, regulatory requirements should be defined so as to ensure the principle of proportionality, in a risk-adequate manner, to prevent any impediments to innovation.
    a. In this respect, German banks propose compiling a catalogue of risks (and corresponding regulatory requirements) that distinguishes providers - both by the products and services they offer and by the systemic risks they represent. For instance, a FinTech which only offers deposits products, and which is not classified as being systemically relevant, might only be required to fulfil requirements regarding product documentation and deposit guarantee schemes (as a FinTech, plus basic IT security requirements). The clearer and more straightforward such a catalogue can be defined, the lower any impediments to innovation will be – and the fairer competition will focus on clients, rather than on regulation.
        i. Such a revision may map the plethora of requirements under individual – and frequently overlapping – regulations (GDPR, ePrivacy Directive and the new proposal for an ePrivacy Regulation, the NIS Directive, the UCPD, the Distance Marketing of Financial Services Directive, PSD, MCD, CCD, PAD, PRIIPS, IDD, MiFIDII/MiFIR, UCITS, AIFMD, EMIR, Solvency II, CRD IV, AMLD) to specific products and services, thus creating a large part of the transparency intended to be achieved through innovation hubs.

  ii. Provided that this catalogue – as noted in the DC – will cover multiple countries as well as multiple industries, it will do justice to current developments, with cross-border providers and cross-sectoral collaboration models.

b. Purely decentralised systems, where there is no provider that might be regulated, remain an issue: it is fair to assume that regulation will have to focus on users – even though such systems also provide for anonymous use. Yet in the absence of any regulatory approach for this, regulating the rest of the playing field would be virtually senseless. For example, money launderers require but one single gap, which is why solutions need to be found as a matter of priority.

What is striking is that key risks identified in Part III B (strategic risk, operational risk, cyber risk, compliance risk) are identified both for established banks and FinTechs, whereas recommendation no. 2 ("Banks should ...") only addresses banks. A uniform approach is required here.

Observations and recommendations: additions and comments regarding the individual chapters of the survey

1) "... the overarching need to ensure safety and soundness and high compliance standards without inhibiting beneficial innovation in the banking sector;"

The general revision of regulatory guidelines – as suggested under 0) above – should involve proportionate and risk-adequate regulatory efforts, depending on the transaction and the provider involved – which would be a perfect example for the stated objective.
We agree with the BCBS's recommendation of a balanced approach and support the European Commission’s three core principles for regulating FinTechs: technological neutrality, proportionality, and market integrity. However, proportionality should be risk-adequate. Applying existing requirements to new entrants – irrespective of business model, type of entity, or type of license – should ensure that the risks of a new entrant’s business activities are fully addressed and monitored. The idea of 'same service, same rules' should be applied to secure consistent standards and fair competition. This is particularly important for standards on cyber-security, AML/CFT, data protection and consumer protection. Regulatory arbitrage must be avoided and the development of a level playing field is essential. We agree with the BCBS that prescriptive standards and rules may create unnecessary barriers to innovation. A principles-based approach (as proposed in chapter 0 above) to regulation should be considered, to allow firms to design risk management programs capable of adapting to the developing financial services landscape.

2) "... the key risks for banks related to fintech developments, including strategic/profitability risks, operational, cyber and compliance risks;"

Whilst this correctly portrays the situation, we would like to ask regulators to not just push regulated institutions to adopt an adequate strategy, but also to call upon states to ensure the international prosecution of cyber-crime, by way of corresponding transnational agreements. We would also like to point out that the regulatory regime – especially concerning AML/CFT – becomes senseless for unregulated players such as BitCoin et al. As pointed out in chapter 0 above, this needs to be resolved as a matter of priority.
We would like to make the following specific comments regarding FinTechs and innovation:

- FinTech innovation does not exclusively occur outside of incumbent banks. Rather, incumbent banks are often an enabler for developing technologies, which helps creates value for the broader economy.
- Innovation may occur through in-house development, as well as through investment in – and partnering with – technology firms and innovators.
- FinTech innovation also allows banks to generate revenues through partnerships.
- However, in order to maintain a level playing field and ensure new market entrants apply proper risk management programmes, regulators should ensure that consistent standards are applied, based on an entity’s business activities.

Regarding cyber risk, we would like to comment as follows:

- The cyber resilience of the financial system requires a robust end-to-end security level across the complete financial services value chain. With increasing interconnectedness and IT interdependencies, a connected system is only as secure as its weakest link.

- Hence, the application of FinTech in financial services must comply with the same high established security standards that incumbent financial services firms must deploy.
- Regulators should actively engage with new and existing market participants, and cyber-security practitioners – to understand emerging trends and address any potential regulatory gaps.
- A cyber-security framework that encourages a risk-based approach, global coordination and sharing of cyber-threat information is critical for continued progress in cyber-security initiatives across all market participants.

3) “Implications for banks of using innovative enabling technologies”

"As far as DLT is concerned"

- We support further efforts to understand the uses and potential risks and benefits arising from the use of DLT.
- Market participants are collaborating on numerous potential approaches to develop effective solutions, which may be used by a broad network of participants.
- Regulators should continue to engage with market participants to understand the implications of such solutions. This will facilitate informed regulatory and supervisory decisions.
- Direct regulatory participation in pilot programmes might help clarify the minimum controls for a DLT-based system to be brought to market. This may include minimum standards on information security, as well as business and design controls.

"In case of Cloud-technology"

- The availability of cloud technology provides clear benefits to firms of all sizes, and will play an important part in the modernisation of bank infrastructure and business models.
- To date, there has been uncertainty concerning the application of existing outsourcing requirements to the cloud services business model; this inhibits broader adoption and materialisation of that model's benefits.
- We strongly support efforts by regulators to provide increased regulatory certainty in this area, such as the EBA’s draft guidelines published in May 2017.
- Regulatory clarity and harmonised standards will not only enable broader adoption by incumbent banks, but will enhance risk management practices for outsourcing across market players of all sizes, and across jurisdictions.
- We encourage regulators to collaborate with cloud services providers and financial institutions, to address potential diverging interpretations on the application of regulatory requirements and to harmonise supervisory expectations.

4) "... the implications for banks of the growing use of third parties, via outsourcing and/or partnerships;"

Especially when compared to the US (Annex 2, page 44) observations 3 and 4 illustrate that it would be beneficial to not only have supervisory authorities regulate these service providers – instead, service providers should be able to apply for 'bank-suitable provider' status, which would enable them to be audited directly. Otherwise, providers that aim to offer their services to multiple banks would not be able to scale their offers – which would burden FinTech – and especially cloud-based – services in Europe. Likewise, to be able to use service providers would require banks to hold immense know-how outside their own area of expertise – a contradiction of the collaborative nature of digitalisation. Outsourcing per se is no (additional) operational risk – see e.g. Jürgen Bott and Udo Milkau: "Outsourcing Risk - a separate operational risk category?" in: Journal of Operational Risk Management, Vol. 10/3, 2017 – therefore, 'sourcing' in general has risk potential, but 'outsourcing' only represents a certain type of sourcing.

Incumbent banks are subject to existing Directives and Delegated Regulations within the EU that provide detailed requirements covering the proper selection, supervision and governance of external service providers to avoid undue additional operational risk. Banks must carefully select external service providers that meet specific performance expectations for the outsourced tasks; banks must design appropriate controls and governance processes to ensure prudent risk management. This includes audits and ongoing supervision by competent supervisory authorities. This framework applies irrespective of the outsourced service or technology. The outsourcing of important operational functions may not be undertaken in such a way as to materially impair the quality of internal controls, and the ability of supervisors to monitor the firm’s compliance with all obligations.

5) "... cross-sectoral cooperation between supervisors and other relevant authorities;"

Needless to say, technology does not only concern banking supervision, but also extends to data protection or cyber resilience of important public infrastructures, for example. Requirements need to be harmonised – for example, security incident reporting obligations differ between regulations, which triggers different reporting requirements to different authorities – leading to complexity and the imposition of administrative burdens.
Observation 5 expands the statement of observations 3 and 4 – also refer to the general comments.

6) "... international cooperation between banking supervisors;"

Observations 5 and 6 show that regulators should adapt a collaborative approach, as employed in the industry, with cross-border and cross-sector collaboration. In this context, particular emphasis should be placed upon finding unique interfaces and homogeneous transitions. This is due to the fact that multiple regulation severely hampers innovation, and – in a worse-case scenario – conflicting requirements would paralyse the industry. This working area should be addressed immediately following the general working area (see above).

7) "... adaptation of the supervisory skillset;"

In our view, this portrays the facts quite accurately: care needs to be taken to ensure adequate remuneration structures. We are competing for the same talent – if only frustrated employees join the public sector, regulators will find it hard to appropriately fulfil their duties.
Ongoing dialogue between regulators and market participants would greatly benefit this effort. Regulators should also ensure that sufficient resources are available to deliver speedy reviews and support responsible innovation. This will become increasingly important as new technology deployment cycles are likely to be much quicker in the future.

8) "...potential opportunities for supervisors to use innovative technologies ("suptech");"

Before tackling the issues referred to (such as AI etc.), we believe considering automated testing methods would provide more – and faster – successes. Using electronic user interfaces and APIs, regulators could carry out numerous controls directly and in an automated manner.

9) "... relevance of existing regulatory frameworks for new innovative business models;"

We would also like to refer to the concept of risk-adjusted, proportional regulation, as outlined above. From the German Banking Industry Committee's perspective, this represents the best possible solution. We need to plug the holes in the system, as a matter of priority, before discussing how finely knit the system should be. Hence, we would like to reiterate the necessity (cf. item 4) for technology providers to subject themselves to a voluntary examination of whether they are ready for banking. Directly subjecting themselves to banking supervision is a necessary option for realising their business models.

10) "... key features of regulatory initiatives set up to facilitate fintech innovation."

Transparency and exchange among national regulators is of great value – but this will not be sufficient: a 'best of breed' approach is necessary to keep up with industry speed. Relief options which have been proven on a national level should be adopted in other countries, after a brief testing period, in order to prevent regulatory arbitrage which would be fatal. In a free market economy, any legislation/regulation should provide guidance to restrict developments which harm other people, or market participants. All other developments are natural developments of free markets, which should be not regulated unless evidence for abuse or misconduct can be provided.
Applying appropriate regulation for FinTech activities inside or outside of banks – and further development of innovative solutions – requires a clear understanding of a solution’s uses, benefits, risks and implementation challenges.
We do not see 'sandboxes' as a form of regulatory relief, but as an option for approaching the highly-regulated financial markets. We see sandboxes and hubs as synonyms – they may be helpful for Fintechs and banks in order to understand regulatory requirements; in turn they may help regulators to understand Fintechs' requirements. The German Banking Industry Committee welcomes the introduction

of this support tool. However, sandboxes or hubs must safeguard investor protection from the very first euro invested, regardless of the regulatory regime a firm is subject to. Applying existing requirements to new entrants – irrespective of business model, type of entity, or type of license – should ensure that the risks of a new entrant's business activities are fully addressed and monitored. The idea of 'same service, same rules' should be applied to secure consistent standards and fair competition. Regulators should be available as a single point of contact for a sandbox or hub, across all areas of activity and fields of law (banking supervision, data protection, consumer protection, …). Temporary scope for decentralised rules should be provided by a uniform European framework.