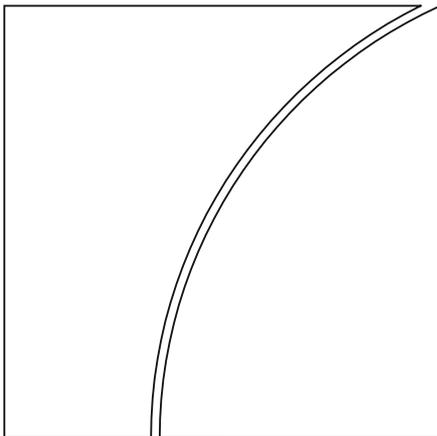


# Financial Stability Institute

## Occasional Paper No 17



### Fintech regulation: how to achieve a level playing field

by Fernando Restoy

February 2021

JEL classification: G18, G21, G28, L41, L51.

Keywords: big techs, competition, financial stability, activity-based regulation, anti-trust, AML/CFT, consumer protection, banks, payment services.



**BANK FOR INTERNATIONAL SETTLEMENTS**

FSI Occasional Papers aim to contribute to international discussions on a wide range of topics of relevance to the financial industry and its regulation and supervision. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based standard-setting bodies.

This publication is available on the BIS website ([www.bis.org](http://www.bis.org)). To contact the BIS Media and Public Relations team, please email [press@bis.org](mailto:press@bis.org). You can sign up for email alerts at [www.bis.org/emailalerts.htm](http://www.bis.org/emailalerts.htm).

© *Bank for International Settlements 2021. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

ISSN 1020-9999 (online)

## Abstract

How regulation should evolve to encourage fair competition between traditional banks and new fintech and big tech players is now being debated. Some advocate moving from an entity-based to an activity-based regulatory approach under the principle "*same activity, same regulation*". However, there is only limited scope for further harmonising the requirements for different players in specific market segments without jeopardising higher-priority policy goals. In fact, there seems to be a strong case for relying more, and not less, on entity-based rules. The regulatory framework should incorporate entity-based requirements for big techs in areas such as competition and operational resilience that would address the risks stemming from the different activities they perform. This strategy would not only help regulation to achieve its primary objectives, but would also serve to mitigate competitive distortions.

## Contents

Section 1. Introduction .....	1
Section 2. The current regulatory framework.....	2
Section 3. Some conceptual preliminaries.....	5
3.1    The relevance of the level playing field objective.....	5
3.2    Activity-based vs entity-based .....	5
3.3    Which regulation should be activity/entity-based? .....	7
3.4    The rationale for the entity-based regulation of banks.....	8
Section 4. Towards a more balanced regulatory framework .....	9
4.1    Is activity-based regulation sufficiently balanced?.....	9
On consumer protection .....	9
On AML/CFT.....	13
4.2    Do we need more entity-based regulation rather than less?.....	14
On operational resilience .....	14
On competition.....	16
Section 5. Conclusions.....	19
References .....	21

# Fintech regulation: how to achieve a level playing field<sup>1</sup>

## Section 1. Introduction

The disruption created by technological progress in the market for financial services arises from (i) an expanded set of services offered to consumers; (ii) the processes and distributional channels followed by firms in offering those services; and (iii) the arrival of new (technological) suppliers of those services.

These developments are bound to generate profound changes in the market structure, as non-bank fintech<sup>2</sup> players are now becoming very active in offering services that in the past were predominantly offered by banks.<sup>3</sup> Their presence in the payment service area is already quite significant. However, they are also gaining weight in the provision of wealth management services, the sale of insurance products and loan underwriting. Those services are increasingly being provided within established technology platforms run by large companies (big techs), where a variety of financial and non-financial products are offered by a plurality of suppliers that may or may not be linked to the platform owner (Frost et al (2019)).

A growing number of products and players increases supply, lowers the cost of financial services and encourages financial inclusion. However, it may also generate risks for the stability and adequate functioning of the financial system.<sup>4</sup>

So far, despite remarkable growth in the recent past, the scale of fintechs' operations is generally limited relative to the overall size of the financial services market. Yet, in some jurisdictions, specific firms (Ant Group in China or Quicken Loans in the United States)<sup>5</sup> have already gained leading market positions. Given significant economies of scale, data superiority and the large scope for network externalities, big techs could very well eventually achieve market dominance (De la Mano and Padilla (2018)).

There is an ongoing worldwide discussion on what the policy approach should be with respect to those market dynamics. Within that discussion, a relevant question is whether the growth potential of fintech and big tech companies could be, in part, the consequence of lighter regulatory requirements compared with those for incumbent players such as commercial banks. This argument could be based on the observation that financial institutions have specific (entity-based) obligations, such as those related to prudential requirements, which do not apply to other competitors in specific markets such as payment

<sup>1</sup> Fernando Restoy, Bank for International Settlements. The views expressed here are solely those of the author and do not necessarily reflect those of the BIS or the Basel-based standard-setting committees. The author is grateful to Claudio Borio, Agustín Carstens, Jaime Caruana, Stijn Claessens, Johannes Ehrentraud, Marcos Fabian, Santiago Fernández de Lis, Jon Frost, Leonardo Gambacorta, Gloria Hervás, Alejandra Kindelán, Jorge Padilla, Andrés Portilla, Jermy Prenio, José María Roldán, Julio Segura and Raihan Zamil for helpful comments and insights. Mathilde Janfils and Aiden Lawson provided outstanding research assistance, and Christina Paavola offered excellent administrative support.

<sup>2</sup> FSB (2017) defines fintech as technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.

<sup>3</sup> See Petralia et al (2019) for a description of the disruption that fintech can create in traditional banking markets. In many cases, fintech players are also offering services in areas currently served by specialised entities such as investment advisers, investment fund managers and insurers.

<sup>4</sup> See Carstens (2018) and FSB (2019).

<sup>5</sup> Ant Group manages the world's largest money market fund (Yu'e Bao) and Quicken Loans is now the highest-growth mortgage lender in the United States. Big tech credit, in particular, is growing rapidly, having reached US\$ 572 billion in 2019 (Cornelli et al (2020)).

services, wealth management or credit underwriting. Regulation specific to banks entail higher compliance costs and can therefore put them at a competitive disadvantage.

The existence of regulatory distortions could violate the principle of *good regulation*, which calls for any public intervention to limit market impact to the minimum required to achieve relevant objectives (OECD (2005)). Unwarranted discrepancies between regulatory requirements for different types of market player could also disrupt banks' activities as intermediaries, thus posing risks to systemic stability (FSB (2019)). Moreover, distorted market developments leading to big tech dominance could threaten competition in the financial services market (BIS (2019)), possibly affecting consumer protection and market integrity.

The banking industry has frequently stressed (eg IIF (2017)) that regulation could promote a level playing field through the adoption of an activity-based approach, as opposed to an entity-based one. That would mean imposing similar requirements upon all active players in a particular market segment, regardless of the legal nature or other characteristics of those entities and, in particular, whether or not they hold a banking licence.

However, entity-based prudential rules for banks are based on specific policy objectives – such as financial stability – that are not subordinated to the achievement of a perfectly competitive landscape. Therefore, level playing field considerations cannot be enough to support a radical overhaul of the current regulatory framework.

At the same time, it could be argued that fintechs – or, more likely, big techs – can also generate concrete threats to relevant policy objectives such as market integrity and stability or fair competition. If that were the case, the introduction of specific rules for those entities, as they exist for banks, would not only contribute to primary policy goals but would also help promote a level playing field.

This paper discusses how level playing field considerations should affect the definition of the regulatory framework following the emergence of fintechs and big techs. It also analyses the extent to which activity-based and entity-based regulations could help achieve socially desirable objectives.

The structure of the rest of the paper is as follows. Section 2 outlines the current regulatory framework for banks and fintech players. Section 3 sets out some considerations that may help in assessing the current framework and the scope for a move towards more activity-based regulation. Section 4 assesses possible adjustments to specific regulations that could help achieve a better balance across different policy objectives. Section 5 concludes.

## Section 2. The current regulatory framework

Banks are subject to prudential obligations that include requirements for minimum capital and liquidity, constraints on large exposures, and specific rules on governance arrangements and compensation schemes for decision-makers. Banks are also subject to additional regulations such as consumer protection, anti-money laundering (AML)/combating the financing of terrorism (CFT) or conduct of business, which apply to the different services they offer, including deposit-taking, credit underwriting, payment services and wealth management.

Prudential requirements for banks take into account all activities that an institution performs. In particular, capital requirements are based on an assessment of the credit, market and operational risk of the institution as a whole. Moreover, the focus of prudential requirements is a financial institution's consolidated balance sheet, sometimes complemented with specific constraints for individual legal entities within banking groups. As a result, all subsidiaries of banking groups are, regardless of what they do, directly and/or indirectly subject to prudential requirements.

Following the emergence of fintechs, no generalised adjustments have been made to the perimeters of financial regulations in order to accommodate their activities as providers of financial services. A few exceptions are the introduction of the category of digital banks in some jurisdictions or regulations on crowdfunding platforms (Ehrentraud et al (2020)). The new regulatory categories for fintechs do not always aim to control the specific risks they pose, but rather sometimes seek to promote increased competition or financial inclusion by imposing (temporarily) lighter requirements.<sup>6</sup>

However, non-banks offering financial services (payments, credit, crowdfunding, wealth management, investment advice, etc) do typically need a licence depending on the activity they perform. As an example, most big techs in the European Union and the United States do hold licences as payment service providers, which are known as *payment institutions* or *e-money institutions* in the former and *money transmitters* in the latter (Table 1). Fintechs offering loans in the United States (eg Quicken Loans) and in China (eg Ant Group) hold non-bank lender licences. So far, fintechs and big techs have not generally sought regular banking licences. There are, however, some exceptions in the EU and the United States.<sup>7</sup> In China, big techs are allowed to own stock in banks, although they should not exceed 30% of the banks' capital. There are several big techs that provide financial services only in partnership with commercial banks.<sup>8</sup>

<sup>6</sup> This is the case in Singapore or Hong Kong SAR, where digital banks are allowed to operate temporarily with more flexible requirements until they reach sufficient scale. In the United States, the Office of the Comptroller of the Currency (OCC) attempted to reduce the barrier to entry in 2018 by creating Special Purpose National Bank Charters for FinTechs, allowing them to circumvent the complex state-by-state licensing method. State banking regulators, specifically the Conference of State Bank Supervisors (CSBS), challenged the legality of these new charters. However, in October 2020 the CSBS issued a new single set of supervisory rules – called CSBS Vision 2020 – that are intended to ease compliance burdens.

<sup>7</sup> An exception in the US is Varo Bank, which obtained a national bank licence in July 2020. Several fintechs in the US have sought to become Industrial Loan Companies (ILCs), as this would allow them to take deposits and obtain Federal Deposit Insurance Corporation (FDIC) insurance. Two of these companies – Square Financial Services and Nelnet Bank – obtained approval in March 2020. ILCs are required to hold significantly higher capital levels than banks, and their parent companies (which are non-banks) must be able to act as “sources of strength” for their depositories.

<sup>8</sup> Examples are the partnership of several banks in Europe with Apple to provide payment services, and the one of Goldman Sachs with Apple to offer Apple Card and with Amazon to provide small business lending. Google is also planning to offer a cheque account product, in conjunction with Citi and other banks. See Cornelli et al (2020) and Crisanto et al (2021).

Licences held by big tech companies in selected jurisdictions

Table 1

Licence held <sup>1</sup>	Licences and presence																	
	European Union			Hong Kong SAR			Brazil			United Kingdom			United States			China		
	P	C	B	P	C	B	P	C	B	P	C	B	P	C	B	P	C	B
Google	✓									✓			✓					
Apple <sup>2</sup>													✓					
Facebook	✓												✓					
Amazon	✓									✓			✓					
Ant Financial	✓			✓		✓	✓+			✓			✓			✓	✓	✓*
Baidu																✓	✓	✓*
JD.com						✓										✓	✓	
Tencent				✓		✓										✓	✓	✓*
NTT Docomo <sup>3</sup>	✓		✓															
Rakuten <sup>3</sup>	✓		✓										✓					
Mercado Libre							✓											

P = payments-related licence. For the European Union, payment institution (PI) or e-money institution (EMI); for Brazil, instituição de pagamento; for the United States, money transmitter, sale of cheques or money services business (governed primarily by state law); for China, third-party payment licence.

C = credit licence. For Hong Kong SAR, money lender licence; for the United States, non-bank lender licence (state-level); for Brazil, sociedade de crédito direto or sociedade de empréstimo entre pessoas; for China, internet microlender or consumer finance licence.

B = banking licence. For the European Union and the United Kingdom, CRD credit institution; for Hong Kong SAR, authorised institution; for Brazil, BCB approval under Resolution 4.122/2012 and Circular 3.649/2013; for the United States, National Bank Charter or state-level Bank Charter (commercial banks, savings banks and trust companies).

✓\* Shareholding of big techs in these banks is limited to 30%.

✓+ Under application.

■ Market presence in partnership or joint venture with other financial institutions (FIs).

<sup>1</sup> The analysis excludes cases in which payments are made and/or credit is extended for purchasing products and services within the platform. Licences shown include those that are (i) included in public registers and (ii) held by big tech entities that trade under the group's trading name.

<sup>2</sup> Apple and Baidu provide payment services in partnership with other FIs in places where they do not hold their own licence. In the case of Apple, partnership consists of providing partner banks with near-field communication technologies for making contactless payments. The Baidu (Du Xiaoman Financial) partnerships with PayPal (2017) and Western Union (2020) aim mainly to facilitate international money transfers.

<sup>3</sup> NTT Docomo set up two subsidiaries that hold licences: DOCOMO Digital Payment Services (EMI licence in Liechtenstein) and net-m privatbank 1891 (CRD CI licence in Germany). Similarly, Rakuten has Rakuten Deutschland GmbH (PI licence in Germany) and Rakuten Europe Bank (CRD CI Institution in Luxembourg).

Source: Crisanto et al (2021).

Under their current licences, big techs and fintechs are subject to regulatory requirements in the areas of consumer protection and AML/CFT. Sometimes, obligations also cover operational (in particular, cyber) resilience. In general, they do not include risk-based prudential requirements as such, beyond the obligation to hold a minimum amount of subscribed capital or own funds.

As regards competition, neither banks nor big techs are subject to specific conditions beyond those derived from general antitrust legislation with respect to cartels, mergers or preventing abuse of market dominance. At the same time, some jurisdictions (the EU, Australia and Mexico) have recently passed open banking legislation aimed at facilitating competition between banks and non-banks in the market for financial services.

## Section 3. Some conceptual preliminaries

### 3.1 The relevance of the level playing field objective

Public policy has an ultimate goal of improving social welfare. Authorities aim at contributing to that objective by targeting intermediate goals such as economic efficiency, financial stability, market integrity or consumer protection. Promoting competitive markets is also one of those intermediate objectives, as it is assumed to foster an efficient allocation of resources and innovation. Policies aiming at ensuring a level playing field among all participants in a particular market constitute one of the instruments available to achieve the competitive markets objective.

Yet specific policy instruments aiming at meeting intermediate policy objectives may have unintended effects on others. Authorities may therefore need to address policy trade-offs, such as the ones existing between financial stability and competition.<sup>9</sup>

In the field of financial regulation, social objectives such as financial stability, market integrity or consumer protection take precedence over favouring competition in financial services markets. In fact, the licensing requirements for those markets typically act as a form of barrier to entry that can only be justified on the basis of higher-priority goals. Moreover, only a minority of financial regulators have a mandate to foster competition and, when they do, as in the case of the Bank of England's Prudential Regulation Authority (PRA), this objective is often subordinated to the primary mission of keeping banks safe and sound (Kirakul et al (2021)).

In the area of competition, the application of specific policy instruments is often made conditional on its proven ability to deliver economic efficiency and favour consumers.<sup>10</sup> Moreover, the complete homogenisation of the requirements to be satisfied by heterogeneous market players (with the aim of achieving a level playing field) may not always lead to more competitive markets. For example, specific controls may be needed for players – such as those with a higher degree of vertical integration – with a greater potential to develop a dominant market position.

Against that background, the achievement of a level playing field (eg between banks and fintechs) should therefore be considered a desirable feature of the regulatory framework only once other higher-priority objectives (including competitive markets) are sure to be met. This effectively creates a *lexicographic order* of objectives.

Thus, analysis of whether regulation may unduly distort the competitive landscape requires a comprehensive assessment. In particular, that analysis should establish whether different requirements for different types of entities performing the same activity could be justified on higher-priority policy grounds – in other words, whether there could be a means of achieving that higher-priority objective with no or less pronounced regulatory discrepancies across different types of entity competing in a particular market segment.

### 3.2 Activity-based vs entity-based

Regulatory requirements for the financial industry can be broadly classified as either activity-based or entity-based. Activity-based rules consist of requirements to be met by all institutions offering a given

<sup>9</sup> See eg OECD (2011) and Vives (2016) for an analysis of the different sources of complementarities and trade-offs between financial stability and competition. In other cases, the hierarchy may not be as obvious, as in the case of possible trade-offs between data portability, which favours competition, and data protection, which favours privacy (BIS (2019)).

<sup>10</sup> For example, Article 101.2 of the European Union Treaty establishes the inapplicability of the anti-cartel provisions in Article 101.1 for agreements or concerted practices "...which contribute to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit...".

service (eg credit underwriting, payment services, investment intermediation, investment advice). Entity-based rules consist of requirements imposed on institutions with a specific licence or charter. That charter is defined in terms of the activities those entities are allowed to perform.

Therefore, what are normally understood as entity-based rules consist of requirements to be satisfied by entities holding a licence that allows them to undertake a particular activity or combination of activities. For example, money service providers in the United States or payment institutions in the European Union are legal persons that are entitled to offer a series of payment services. Similarly, institutions subject to bank prudential regulation are entities called “banks” in the US and “credit institutions” in the EU. In both cases, those entities are defined, based on the activities they are allowed to perform, as institutions that may take deposits and give credit.

The distinction between activity-based and entity-based rules is only relevant as long as entities perform different types of regulated activities. In fact, if all regulated entities performed only one regulated service (say, payment services or credit underwriting), rules to be satisfied by those entities would coincide, by construction, with those governing the provision of that service.

The situation is different, however, when entities perform a combination of regulated activities and that combination is considered to generate risks for the achievement of primary policy objectives. As those risks cannot be addressed by an activity-by-activity approach, they require imposing entity-based obligations on firms performing such a combination of activities. That is the justification, for example, of the limits imposed on audit companies to perform also consultancy services or, as will be seen later, of the prudential rules addressing the risk transformation that banks perform by combining deposit-taking with risky investment.

Most regulatory frameworks for the financial sector contain both activity- and entity-based-rules. In fact, alongside imposing requirements on firms interested in offering a specific financial service, regulations often authorise entities already holding a different licence – and that are subject to their own entity-based obligations – to perform that activity.<sup>11</sup> The result is that a specific financial service could be offered by firms that are not subject to the same entity-based rules. To the extent that entity-based rules influence the competitive conditions under which they can offer a service, they unlevel the playing field for that particular activity.

The key question is therefore whether or not, and under what circumstances, it would be justified to harmonise all requirements for all authorised providers of a specific product or service (eg payment services). That would entail either imposing the most comprehensive entity-based (eg prudential) restrictions on all firms allowed to perform a specific activity or avoiding entity-based restrictions that affect only a subset of competitors (eg banks) in that specific market.

The first approach would mean, at the very least, requiring a bank licence for all firms allowed to compete in markets in which banks also participate. The second approach would entail breaking up entity-based rules into specific requirements associated with each of the activities performed. Entities performing more than one activity – for instance, by employing different subsidiaries – would simply need their subsidiaries to satisfy the requirements imposed for each activity.

The *lexicographic order* of objectives for regulation described above helps shed light on whether either of those two approaches could be justified. According to the hierarchy, facilitating a level playing field is considered an objective of regulation even though it ranks below promoting financial stability and other primary goals.

The first option would mean imposing upon all providers of a specific activity a number of requirements which are only warranted – on higher-priority policy grounds – for a subset of entities that perform other activities as well, such as banks. Unless it is proven otherwise, that extension of entity-based

<sup>11</sup> For example, PSD2 establishes the licence of a “payment institution” in the EU but also allows other licences, such as e-money and credit institutions, to perform the same functions.

requirements to all players would not be necessary to achieve primary policy objectives, such as financial stability. It does, however, damage the level playing field, as it would simply protect a subset of firms from their competitors. This option therefore fails the *lexicographic order* test.

The second (more activity-based) approach facilitates the harmonisation of competitive conditions for all types of player. Yet, as achieving a level playing field is subordinated to other public policy goals, the extent to which that approach is warranted should be decided based on its impact on the primary objectives of regulation.

In particular, it is necessary to ascertain whether those primary objectives can be achieved by introducing rules for performing each activity, or whether there could be risks or challenges that emerge from the combination of activities that specific entities perform. That assessment requires separately analysing regulations aimed at achieving different policy objectives.

### 3.3 Which regulation should be activity/entity-based?

Depending on the objectives pursued by different regulations, an activity-based, an entity-based or a mixed approach may be required.

On the one hand, there are regulatory areas for which an activity-based approach could be sufficient in order to achieve the relevant objectives, such as consumer protection or AML/CFT.

Rules for the protection of consumers of financial products include transparency obligations, mobility across providers, pricing policies, responsible publicity for financial products, and fitness and suitability assessments. While specific requirements may vary across products/activities, there seems to be little reason to impose heterogeneous rules upon different providers of a particular service, even if they also perform other activities.<sup>12</sup>

AML/CFT requirements comprise mainly customer due diligence (CDD), record-keeping and reporting obligations for suspicious transactions. In principle, there are no obvious risks to market integrity emerging from the provision of a combination of different types of financial service that would merit special entity-based rules.

On the other hand, prudential regulation aims to address the impact of the failure of specific institutions on the stability of the system. To the extent that these risks stem from the vulnerability of those institutions' balance sheets, prudential regulation should follow an entity-based approach. In particular, it needs to establish specific requirements for entities – such as banks – which perform a combination of activities that entail risk transformation: taking government-protected liabilities redeemable at short notice and at par value (deposits), and investing those funds in risky, longer-term and less liquid assets (eg credit).

There are, finally, other regulations that may require a combination of activity-based and entity-based rules. Such is the case for regulations on operational resilience, which include provisions related to cyber security, business continuity and third-party providers. The significance of an operational incident in a particular firm is a function of the activity it performs. Yet, for firms that perform several different activities, an operational incident in a specific business line may impact the continuation of other activities. If those disruptions have a sufficiently large potential impact on the economic or the financial system, they justify the introduction of entity-based rules. The most obvious example is that of banks, where the integration of systems used to offer different services to clients may justify specific rules. Yet entity-based rules could also be warranted for other large non-bank (big tech) platforms offering a wide array of services to a large set of agents that includes financial institutions (eg cloud services).

<sup>12</sup> Note that, for the sake of simplicity, consumer protection rules mentioned in the text do not include those regarding conduct of business. The latter often entail limitations and restrictions for firms conducting related activities (such as investment advice and securities intermediation or audit and consultancy services). Those rules would certainly enter the entity-based regulation category.

Competition is also an area where a combination of activity-based and entity-based rules seems appropriate. The regulatory framework in this domain covers, mainly, the prevention of cartels, conditions for mergers and acquisitions, and controls to prevent abuse of market dominance. The first two components may be well served using general principles for all sectors and some sector-specific rules for traditionally regulated sectors. But, importantly, preventing abuse of market dominance does require a more entity-based approach, as anti-competitive practices may emerge from the way firms combine the different activities they perform. Abuse may occur when firms use their dominant position in a particular market to reduce competition in other related markets. This may occur, for example, when entities in the market of a particular product also compete in the market of complementary goods or services or in the market for the inputs required to offer that product.

### 3.4 The rationale for the entity-based regulation of banks

Prudential regulation focuses on the consolidated balance sheet of financial institutions. That implies that the separation of the different activities performed into different subsidiaries does not have a material impact on prudential requirements.

The focus of prudential rules on consolidated balance sheets derives from Principle 12 of the *Core Principles for Effective Banking Supervision*, which requires “adequately monitoring and, as appropriate, applying prudential standards to all aspects of the business conducted by the banking group worldwide”. This includes the supervisor’s ability “to identify and act upon risks posed by unregulated activities within the group to the regulated entity or to financial stability” (BCBS (2016b)). The idea is that, even when activities are separated into different legal entities, the core activities of the bank are not sufficiently protected from risks stemming from ancillary functions.

Therefore, non-deposit-taking subsidiaries of banking groups specialised in ancillary services are subject to a regulatory burden which is not imposed on other, independent firms performing the same function. That may be seen as penalising their competitive position when they offer services also provided by non-banks. At the same time, it could be argued that banks’ ability to provide a suite of services (including deposit-taking) constitutes a competitive advantage over non-banks offering only a subset of those services, for which a banking licence is not required. Moreover, non-banks may sometimes need to comply with restrictions which are not imposed on banks. For instance, payment service providers other than banks typically need to ensure the insulation of clients’ funds from the rest of their liabilities.<sup>13</sup> These elements may mitigate the impact of banks’ entity-based regulation on the level playing field in the market for some financial services.

In any case, the main rationale of the current regulatory approach is that the safety and soundness of each institution depend on all the activities it performs and the way they interact with each other. To the extent that the combination of those activities creates risks beyond the sum of those associated with each of the activities, a group-wide entity-based approach is warranted.

The case for a group-wide approach to prudential regulation has strengthened following the Great Financial Crisis of 2007–09. The crisis showed that a bank’s poor performance when conducting non-core activities, making excessively risky investments in banks’ own accounts or sponsoring off-balance sheet securitisation vehicles could trigger a crisis for the whole group. This can thereby affect its ability to perform core functions. Indeed, post-crisis reforms have introduced not only more stringent requirements at the consolidated level, but also additional (structural) measures to further protect banks’ core activities

<sup>13</sup> An extreme example is seen in China, where the People’s Bank of China has imposed a 100% reserve requirement for clients’ balances at non-bank payment institutions, such as Ant Group’s AliPay and Tencent’s WeChat Pay.

from risks stemming from other functions.<sup>14</sup> Moreover, supervisors have obtained the power to monitor and require banks to control risks arising from activities that may eventually affect them even if they are performed by entities that do not belong to their consolidated perimeter.<sup>15</sup>

Against that background, exempting non-deposit-taking subsidiaries of banking groups from the prudential regulatory perimeter is not consistent with prudential regulation's primary objective of preserving financial stability. This does not necessarily mean that all prudential requirements should be imposed mechanically on all subsidiaries at the solo level, regardless of the activity these perform and the scale of the operations they undertake. The principle of proportionality should be applied, particularly for non-deposit-taking subsidiaries, for which individual requirements should be based on their contribution to the risk profile of the group as a whole.

## Section 4. Towards a more balanced regulatory framework

The previous sections suggest that, in order to achieve relevant policy objectives in accordance with the proposed hierarchy, regulation should adopt a combination of activity- and entity-based rules.<sup>16</sup> Therefore, not all firms competing in a particular market segment should necessarily be subject to the same rules. Differences in regulatory requirements should, however, be justified on the basis of higher-priority policy objectives. Provided these higher-priority policy objectives are achieved, regulation should aim to minimise gaps in the regulatory burdens faced by different players.

As a result, potential sources of unwarranted competitive distortions would normally be of two types: (i) asymmetric requirements for different players under regulations that should follow an activity-based approach; and (ii) a lack of entity-based obligations for non-banks when warranted on primary policy grounds. This section reviews whether existing regulation may generate either of these two types of distortions.

### 4.1 Is activity-based regulation sufficiently balanced?

As discussed in Section 3, for regulation in areas such as consumer protection or AML/CFT, there does not seem to be a strong case for requiring substantially different rules for different types of entities performing a specific activity. The section below assesses whether this is currently the case.

#### On consumer protection

In general, existing requirements in the consumer protection domain in relation to the provision of payment services, credit underwriting, securities services and wealth management are substantively similar for all players allowed to perform those activities.

In the area of payment services, regulation covers obligations related to transparency of services and fees, mobility of accounts across providers, conditions for authorisation and execution of orders, and data protection. In the area of lending, rules affect the transparency of terms and conditions, non-discriminatory accessibility criteria, tests of affordability, transmission of information to third parties, etc. In the area of securities services and wealth management, it includes information requirements,

<sup>14</sup> Those are the structural measures undertaken in the United States under the Dodd-Frank Act (Volcker rule) and the ring-fencing obligations in the United Kingdom (following the Vickers Report).

<sup>15</sup> These are the measures to address step-in risks. See BCBS (2017).

<sup>16</sup> In other words, activity-based and entity-based regulation should be seen as complementary rather than as substitutes (Restoy (2019)).

suitability tests, obligation to act in customers' interests, etc. In general, all requirements in these areas apply widely to different types of providers of each service.

For example, in the European Union, the Payment Accounts Directive (Directive 2014/92/EU) and the Payment Service Directive (Directive (EU) 2015/2366 or PSD2) contain consumer protection provisions which apply to a wide variety of regulated providers, including credit institutions, e-money institutions and payment institutions (Box 1). In the United States, payment services are regulated by state law (Box 2). Yet all providers of payment services in the US are subject to the jurisdiction of the Consumer Financial Protection Bureau (CFPB),<sup>17</sup> which issues rules, monitors compliance and takes enforcement actions. In addition, states can issue their own requirements in the area of consumer protection, which are often more stringent than federal rules. These are applied to all firms active in their jurisdiction, including state-registered banks and thrifts and subsidiaries of national banks.

Box 1

## Payment service providers in the European Union

The regulation of payment services in the EU is covered in the EU's Payment Service Directives (Directive 2015/2366 or PSD2). PSD2 covers the following activities:

1. Services enabling cash to be placed in a payment account as well as all the operations required to operate a payment account.
2. Services enabling cash withdrawals from a payment account as well as all the operations required to operate a payment account.
3. Execution of payment transactions, including transfers of funds in a payment account with the user's payment service provider or with another payment service provider.
4. Execution of payment transactions in which the funds are covered by a credit line for a payment service user.
5. Issue of payment instruments and/or acquisition of payment transactions.
6. Money remittance.
7. Payment initiation services.
8. Account information services.

The provision of those services is subject to a number of activity-based rules. These include conditions for access to services, transparency of conditions and information requirements for payment services, clients' consent, providers' liabilities, execution time and value date, data protection, operational and security risks, incidence reporting and authentication procedures.

Authorised providers of payment services include *payment institutions*, *electronic money (e-money) institutions* and *credit institutions*.<sup>①</sup> All of them are subject to their own entity-based rules. In particular:

A **payment institution** is defined in Article 4 of PSD2 as a legal person that has been granted authorisation to provide and execute payment services (the ones outlined above).

These institutions are subject to obligations regarding initial capital, ongoing own funds, control of shareholding, internal control, mechanisms to safeguard clients' funds, data protection, business continuity and the handling of incidents and complaints, etc.

<sup>17</sup> The CFPB was created by the Dodd-Frank Act to "provide a single point of accountability for enforcing federal consumer financial laws and protecting consumers in the financial marketplace. Before, that responsibility was divided among several agencies".

An **e-money institution** is defined in Article 2 of Directive 2005/60/EC (E-money Directive) as a legal person that has been granted authorisation to issue electronic money. This is defined as electronically (including magnetically) stored monetary value, as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer. Unlike payment institutions, which do not issue any means for payments, e-money institutions do issue claims, in exchange for cash which is used to process payments.

As a result, e-money institutions are subject to stricter requirements in terms of initial capital and own funds. They must also satisfy strict requirements for investment of the funds received in exchange for e-money and to ensure the redeemability, at any moment and at par value, of the monetary value of the electronic money held.

① In its definition of payment service providers, the Directive also includes post office giro institutions, the ECB, national central banks and national, regional or local authorities not acting in their capacity as public authorities.

Box 2

## Money transmitter licensing in the United States

Many fintech and big tech firms in the United States hold licences as Money Transmitters (MTs). MTs are a specific type of money service business (MSB) that both accept *and* transmit “currency, funds or other value that substitutes as currency” to and from various locations or people through channels including (but not limited to) banks, electronic funds transfer networks or informal value transfer systems.

Registration must take place with the designated agency in each state in which they are active. However, as an MSB, money transmitters are also expected to register with FinCEN 180 days after being established, and these registrations must be renewed every two years. They must also comply with AML/CFT and consumer protection regulations issued by FinCEN and the CFPB, respectively. MTs are also subject to federal requirements on financial integrity, consumer privacy and cyber resilience. In most cases, states have the option of imposing more stringent requirements, such as when New York passed its own cyber security framework or when California passed its Consumer Privacy Act.

As of 2019, 45 state agencies manage over 5,700 money transmitter licences for over 450 companies via the Nationwide Multistate Licensing System (NMLS). Forty-nine of the 50 states have their own unique money transmitter licence (MTL) requirements. Montana does not require money transmitters to be licensed.

Generally, MT requirements can be broken up into the following elements: management, governance, financial risk, liquidity and capitalisation. State licensing requirements typically require the names, locations and, in some cases, background checks of a company’s proprietors and executive officers. A company may also need to provide information on its structure and operations across state lines. MTs are also required to renew their licences annually or every other year. Some states offer “reciprocity” by allowing money transmitters licensed in their states to operate in other states with similar legal frameworks.

MTs are required to have some form of surety bond. This amount can vary from as little as \$10,000 to up to \$7,000,000 depending on the size and scope of the business in question. Five states – California, Georgia, Missouri, Montana and New York – do not have any minimum net worth requirements. Net worth requirements range from \$1,000 to \$3,000,000 and are either a flat amount or structured such that they will increase as a money transmitter grows its business. State regulations also stipulate that money transmitters must maintain a certain level of “permissible investments” – primarily highly rated, liquid assets – that are equal to the value of their outstanding obligations. While these requirements are key to ensuring the safety of consumer funds, the treatment of specific assets varies across states.

MTs are examined annually by state regulators, who review operational resilience, financial condition, management, AML/CFT compliance and internal controls. Reviews can be conducted by individual regulators or by multistate teams if the transmitter is operating in states that have harmonised regulatory requirements. Licensees must submit regular financial statement reports, comply with permissible investment adequacy regulations, and disclose all branch and agency listings.

In an effort to harmonise licensing requirements, the Conference of State Bank Supervisors (CSBS) developed its NMLS in 2008. The NMLS was designed as a “one-stop shop” for MSBs with operations in different states to apply, amend, update or renew their licences for different states via a single set of uniform applications. Currently, 28 states are using the NMLS to offer multistate money transmitter licences via its Multistate MSB Licensing Agreement Program. The Uniform Money Services Act (UMSA), unveiled by the Uniform Law Commission, defined a clear safety and soundness framework that connected all MSBs, with the goal of encouraging states to adopt it. Twelve states have adopted some form of the UMSA. The CSBS published a “MSB Model Law” in 2017 that was based on the UMSA. The Model Law prioritises consumer protection, “bad actor” prevention, and coordination between state regulators to preserve safety and soundness. Finally, the law provides proposals for standardising net worth, surety bond and permissible investment requirements. It also provides alternatives for ensuring ample capital and liquidity.

In the area of credit underwriting, the EU Directives on Consumer Credit (Directive 2008/748/EC) and on Mortgage Credit (2014/17/EU) establish rules that must be met by all “creditors”. The same applies, in the United States, to the Equal Opportunity Act, the Home Mortgage Disclosure Act and the Truth in Lending Act.

Finally, in the area of securities services and wealth management, consumer protection rules are imposed on all professional asset managers. For example, in the EU, this activity is regulated under the MiFID Directive, which contains provisions that apply to banks and non-banks in a similar fashion. In the US, the Securities and Exchange Commission (SEC) has, since 1934, had broad regulatory and enforcement authority over all capital market participants in order to protect investors, among other objectives.<sup>18</sup>

Therefore, fintech and big tech providers of payment services, credit or wealth management services are, in general, subject to consumer protection rules similar to those applied to banks.<sup>19</sup>

Despite the lack of clear examples of explicit differentiation between consumer protection rules for banks and non-banks performing the same activity, there could be significant differences in application and enforcement criteria. Those differences may be pronounced for activities that do not require licensing or registration, as is the case for credit underwriting in a number of European jurisdictions.<sup>20</sup> Moreover, many of the above rules are subject to some form of proportionality, which implies lighter obligations for small firms or for small-volume operations. However, the small size of non-registered lenders and firms benefiting from proportionality rules makes them hardly relevant from a competition point of view.

Probably more relevant are the different procedures followed for oversight and enforcement of activity-specific consumer protection rules.<sup>21</sup> Discrepancies could more easily emerge in jurisdictions

<sup>18</sup> The passage of the National Securities Market Improvement Act (NSMIA) in 1996 gave the SEC the authority to pre-empt state-level “blue sky” regulations for certain types of securities, thus requiring more types of securities offerings to comply with its activity-based requirements. State securities regulators may still impose additional requirements for securities not covered by NSMIA and for smaller firms, or those that manage \$100 million or less.

<sup>19</sup> Recently, regulators with consumer protection responsibilities around the globe have issued warnings, guidance and, sometimes, bans affecting crypto-asset-related service providers (Ehrentraud et al (2020)). The regulatory framework may, however, need to be adjusted to ensure that those activities are fully covered by effective consumer protection rules. In the EU, there is already a legislative proposal aimed at adjusting the regulatory perimeter to incorporate crypto-asset-related activities (EC (2020a)).

<sup>20</sup> This is actually the case in all EU member states except Austria and Germany. In the United States, mortgage lending is a reserved activity, and licences are issued at the state level.

<sup>21</sup> Recent developments point to an intensification of the supervisory scrutiny of big techs. On 26 December 2020 the People’s Bank of China (PBC) and other relevant domestic regulatory agencies held regulatory talks with Ant Financial Group. As part of the discussions, agencies imposed specific requirements on Ant to rectify identified deficiencies: these include, but are not limited to, the following elements: improve trading transparency; refrain from unfair competition; operate the personal credit reporting business on a licensed basis in compliance with laws and regulations; protect the privacy of personal data; improve corporate governance and follow applicable regulatory requirements related to its lending, insurance, wealth management and

where financial oversight is organised by sector, ie where different supervisors monitor compliance with all rules affecting entities belonging to each sector, eg banks, payment institutions, insurance companies, securities firms. In these cases, supervisory guidance, expectations and intensity may vary for entities monitored by different supervisors. That could, in practice, imply more specific and, possibly, more stringent requirements for institutions that are subject to more intrusive oversight, such as banks.

From that point of view, the objective of ensuring a homogeneous application of consumer protection rules across different types of entity is better served by a functional (eg twin peaks) model (Calvo et al (2018)) rather than supervision organised by sector. In particular, a unified consumer protection agency for all types of financial product – such as the CFPB in the United States – fits that goal well.

## On AML/CFT

International standards on AML/CFT apply to a broad definition of *financial institutions* that include a large variety of financial service providers.<sup>22</sup> Moreover, the Financial Action Task Force (FATF) has already adjusted its standards to incorporate all entities involved in crypto-asset-related activities, including stablecoins (FATF (2020)).

The standards establish stringent rules for financial service providers, particularly in relation to customer due diligence, record-keeping and the reporting of suspicious transactions. Following FATF principles, national regulations (eg the Bank Secrecy Act in the US and the AML Directive in the EU (AMLD5)) contain obligations that apply to nearly all types of entity offering financial services.

However, as in the case of consumer protection, AML/CFT requirements are not always sufficiently prescriptive and can therefore lead to different applications by different entities (BCBS (2016a)). That is particularly the case for CDD requirements. It is generally accepted that onboarding processes are typically more thorough when clients want to open an account with a credit institution than when they operate with other players, such as e-money institutions or other payment service providers, even if all those institutions need to comply with the same AML/CFT legislation.<sup>23</sup>

The overwhelming difficulty of supervising all financial transactions that could be conducted to transfer funds with illegal purposes obliges supervisory authorities to prioritise their oversight activities. This risk-based approach, which is part of FATF principles, also helps mitigate the impact of AML/CFT provisions on the supply of financial services for the underserved population, particularly in jurisdictions that lack a robust personal identification regime.

In practice, the application of this risk-based approach tends to attach higher supervisory scrutiny to operations conducted by banks, as opposed to those performed by other account providers. This is partly due to the larger volume of banks' transactions compared with those initiated by other players. Moreover, absent a suitable store-of-value alternative, bank accounts are normally part of the travel route of most transfers of money.

More stringent supervisory scrutiny and frequent enforcement actions involving severe penalties have, in practice, triggered the application by banks of AML/CFT criteria that are more stringent than those

securities business; and to establish a financial holding company and implement regulatory requirements to ensure capital adequacy and compliance with related party transactions. See PBC (2020).

<sup>22</sup> These include acceptance of deposits and other repayable funds from the public; lending, financial leasing, money or value transfer services; issuing and managing means of payment; financial guarantees and commitments; trading in money market, foreign exchange, securities and futures; participation in securities issues and the provision of financial services related to such issues; individual and collective portfolio management; safekeeping and administration of cash or liquid securities on behalf of other persons; investing, administering or managing funds or money on behalf of other persons; underwriting and placement of life insurance and other investment-related insurance; and money and currency changing.

<sup>23</sup> See Thomson Reuters Legal (2018), Blank Rome (2018) and ACAMS (2019).

of fintechs. Banks' internal procedures often follow specific guidance issued by banking regulators, international standard setters<sup>24</sup> and industry bodies such as the Wolfsberg Group.<sup>25</sup>

However, as the importance of non-bank providers of financial services grows, especially fintechs, this gap in the rigour with which rules are applied may further test the effectiveness of the AML/CFT framework and pose increased risks to market integrity (Stone (2020)).<sup>26</sup> Moreover, it penalises the competitive position of banks by imposing a more costly regulatory burden on them compared with their non-bank competitors.

The preservation of both market integrity, as a primary objective, and the minimisation of market distortions supports the need to ensure an equally effective monitoring of compliance with AML/CFT rules for all players. In addition, further efforts, including additional regulatory adjustments, may be required in some domains where new players are active. This is the case for crypto-asset-related transactions, particularly if conducted on decentralised platforms that allow for peer transactions with unhosted wallets (FATF (2020)).<sup>27</sup>

## 4.2 Do we need more entity-based regulation rather than less?

Section 3.4 argued that an entity-based approach for banking regulation is fully warranted given that the combination of activities that banks perform involves socially relevant risks that cannot be fully addressed by imposing specific requirements on each of the services they provide. In particular, prudential regulation aims to mitigate financial stability risks stemming from the maturity, liquidity and other risk transformations that banks perform by combining different activities.

To the extent that other entities – such as fintechs and big techs – do not perform risk transformation activities as such, it would not be warranted to impose on them prudential requirements akin to the ones banks have to satisfy. Yet there are other areas, such as operational resilience or competition, for which an entity-based approach could also be justified (in combination with activity-based rules) not only for banks but also for other providers of financial services.

### On operational resilience

Ensuring the continuous and adequate performance of business operations by financial institutions is an important ingredient in the regulatory framework. In the case of banks, operational risk is a factor affecting capital requirements in international prudential standards. Yet the notion of operational risk in the Basel standards is relatively narrow, as it refers to pecuniary costs or penalties resulting from banks' operations.<sup>28</sup> The concept of operational resilience is much broader, as it includes all factors affecting entities' abilities to deliver critical operations (BCBS (2020b)). Therefore, operational resilience cannot be determined by banks' capacity to mitigate operational risk in the narrow sense of prudential standards. More importantly, instruments for promoting operational resilience go substantially beyond capital requirements to cover operational risk.

<sup>24</sup> See BCBS (2016a, 2020a).

<sup>25</sup> The Wolfsberg Group is an association of 13 global banks which aims to develop frameworks and guidance for the management of financial crime risks.

<sup>26</sup> The first relevant enforcement action for non-banks in the United States took place in 2015, with the imposition by FinCen of a \$700,000 penalty against a digital currency operator that was found not to have an adequate AML programme.

<sup>27</sup> See also Arner et al (2020) for a discussion on the risks posed by this type of transaction.

<sup>28</sup> More concretely, the Basel Committee on Banking Supervision (BCBS) defines operational risk as "risk of possible loss resulting from inadequate or failed internal processes, people and systems or from external events" (BCBS (2011)).

International standard-setting bodies<sup>29</sup> have introduced high-level principles for specific financial institutions (such as banks, insurance companies and market infrastructures) that deal with specific aspects of the wider concept of operational resilience, such as outsourcing, business continuity and cyber security.<sup>30</sup> There are, however, no comparable international standards for payment service providers.

Of special relevance to the provision of technology-intensive financial products and services are the existing rules related to the provision of services by third parties. In several jurisdictions, including the United States, requirements are substantially more detailed in the case of banks<sup>31</sup> than for other firms.

In the European Union, outsourcing is regulated for banks under the Capital Requirements Directive (CRD), for payment and e-money institutions under PSD2, and for providers of investment services under MiFID2. Moreover, there are guidelines (issued by the European Banking Authority) which are binding for all regulated institutions. The imposition of requirements at the subsidiary level and the consideration of services provided by other subsidiaries within the group as outsourcing may make the rules particularly stringent in the case of banks.

Only recently, regulators have started to adopt a more comprehensive approach that entails identifying all the various dimensions of the concept of operational resilience, the introduction of a specific and consistent set of requirements for incident prevention and recovery, and the expansion of the set of entities subject to the new rules.<sup>32</sup> Moreover, those initiatives adopt a sound application of the principle of proportionality that implies particularly stringent requirements for big market operators, regardless of their legal nature or statute.

It seems, therefore, that regulation fostering operational resilience is evolving towards a framework characterised by two components: (i) capital requirements for entities subject to prudential regulation as a function of their operational risk; and (ii) comparable requirements to ensure adequate prevention and management of operational incidents for all providers of financial services. This framework, once completed, will constitute a step forward in delivering operational resilience objectives while facilitating a more level playing field.

Yet it remains to be seen whether a more stringent entity-based approach may be necessary for big non-bank players (big techs). In particular, operational incidents on platforms offering a wide range of financial and non-financial services may generate systemic (and possibly also global) disruptions. This may deserve ad hoc regulatory attention and, eventually, the expansion of the notion of what is considered "systemic", which currently applies, in practice, only to traditional financial institutions or market infrastructures<sup>33</sup> so that it includes this type of firm. A related challenge would be the monitoring of operational resilience safeguards that could be introduced for big techs with a global scope of operations. This requires the current arrangements for cross-border regulatory and supervisory cooperation to be strengthened significantly.

<sup>29</sup> See eg BCBS (2020b).

<sup>30</sup> See Joint Forum (2005, 2006) and FSB (2018).

<sup>31</sup> See FDIC (2008), Federal Reserve (2013) and OCC (2013).

<sup>32</sup> See Bank of England et al (2019), European Commission (2019), FFIEC (2019), Monetary Authority of Singapore (2020) and IOSCO (2020).

<sup>33</sup> At present, the notion of what is considered "systemic" in international regulatory standards is exclusively applied to traditional financial institutions, such as banks and insurance companies, and to market infrastructures. In the United States, there exists a procedure for a designation by the Financial Service Oversight Council (FSOC) of non-bank institutions as "systemic". That procedure has been applied only once to a non-bank and non-insurance company. This was the case of GE Capital between 2013 and 2016. The criteria used for that designation stressed, however, the significant interconnection between traditional financial intermediaries through their financing activities and funding model (FSOC (2013)).

A connected debate is on the regulatory treatment of cloud service providers (CSPs), some of which (like Google or Amazon) are linked to big techs offering a wide range of financial and non-financial services. Given the increasing reliance by both financial and non-financial firms on cloud services, a significant incident affecting the security or the operational continuity of CSPs may have potentially large systemic effects. The services that CSPs offer to financial institutions are subject to the outsourcing controls imposed by financial regulation. Yet so far there are no specific rules and standards on CSPs themselves. Recently, a debate has emerged in the United States on whether large CSPs should be designated by the Financial Service Oversight Council (FSOC) as systematically important financial market utilities (SIFMUs).<sup>34</sup> That would entail CSPs being subject to ongoing monitoring and specific requirements affecting governance, operational risk management and recovery planning. Yet that designation would, in principle, affect only the legal entity providing cloud services and not the parent (big tech) company.

## On competition

Regulatory frameworks for promoting competition in the economic system normally comprise three instruments: (i) a primary law containing general principles and high-level rules to address cartels, or concerted practices, mergers and acquisitions, and to prevent the abuse of market dominance;<sup>35</sup> (ii) case law establishing criteria for the application of the general principles in formal law to specific situations; and (iii) specific regulation to be satisfied by all firms operating in a particular sector.<sup>36</sup> There is, therefore, no specific entity-based regulation in the area of competition. The existing legal framework contains, in principle, sufficient grounds for controlling anti-competitive practices, including the abuse of market dominance, by any type of entity.

Big tech platforms may pose significant risks to fair competition. Their business model entails significant network externalities, ie platforms attract more consumers as the number of sellers increases and vice versa. Together with substantial economies of scale (given the intensive use of technology), this produces a natural tendency on the part of successful platforms to grow increasingly large and to offer a wide array of services. That explains why platforms originally specialised in e-commerce and advertising have often quickly proceeded to offer payment services and, in some cases, to sell insurance, offer wealth management vehicles or grant loans, among other financial and non-financial services.

These trends – which can lead to market dominance – are intensified by the economies generated by the accumulation of data on platform participants. That data superiority helps improve the supply of services and attract buyers, and therefore sellers, as a result of network externalities.

Market dominance can give rise to different types of anti-competitive practices. These include the establishment of preferential treatment for sellers affiliated with the platform, bundling of different services, personal data misuse, cross-subsidisation of products, and discriminatory access conditions for participants.

In principle, all these practices can be subject to penalties derived from the application of competition law, provided harm to consumers is proved.<sup>37</sup> Still, some modifications may need to be

<sup>34</sup> See Fratto and Reiners (2019), IIF (2019) and the letter on the matter from two Democratic lawmakers to the US Treasury Secretary (Porter and Velázquez (2020)).

<sup>35</sup> These aspects have been regulated in the United States since the Sherman Act (1890) and Clayton Act (1915). In the European Union, they are covered in Articles 101 and 102 of the EU Treaty.

<sup>36</sup> In the European Union, specific competition regulation exists for the following sectors: agriculture, insurance, motor vehicles, postal services, transport and electronic communication. See EC (2013).

<sup>37</sup> In the European Union for example, authorities have since 2017 imposed three fines totalling €8.25 billion on Google for anti-competitive behaviour. In 2020, they opened a series of investigations on possible anti-competitive practices by Apple and Amazon. The former was alleged to have made illegal use of non-public business data and to have favoured vendors using

introduced to existing legislation in order to ensure that anti-competitive behaviour by big techs is repressed.<sup>38</sup>

In any case, an approach based purely on general antitrust law may not be enough to prevent the potentially damaging effects on competition that the abuse of market dominance by big techs could generate. Antitrust enforcement actions are typically slow, and the standard of proof requested is very stringent. This may leave disruptive anti-competitive practices unsanctioned either indefinitely or until it is too late to reverse their adverse effects on competitors (De la Mano and Padilla (2018)).

There thus seems to be a case for considering the establishment of specific entity-based regulations for big tech platforms that would complement general competition law by restricting ex ante certain practices that could be considered anti-competitive. This is the approach currently under discussion in the US House of Representatives,<sup>39</sup> the European Union<sup>40</sup> and China (Box 3).

other Amazon services. The latter, already sanctioned in 2018, introduced payment devices on its iPhones that were reserved exclusively to ApplePay. In October 2020, the US Department of Justice initiated actions against Google for “anticompetitive and exclusionary practices in the search advertising markets”. In December 2020, the Federal Trade Commission issued a *complaint* against Facebook for “illegally maintaining its personal networking monopoly” following the acquisition of WhatsApp and Instagram.

<sup>38</sup> For example, the German Finance Ministry has proposed the inclusion of the notion of intermediation power that could be used to act against platforms that unduly restrict access to platforms of specific vendors. Other reforms could include modification of the standard of proof in order to counter strategies aimed at reducing competitive pressure, even if harm to consumer welfare cannot be proved (Crémer et al (2019)).

<sup>39</sup> The US House of Representatives Subcommittee on Antitrust, Commercial and Administrative Law released an antitrust report in October 2020. The purpose of the investigation behind the report was to “(1) document competition problems in digital markets; (2) examine whether dominant firms are engaging in anti-competitive conduct; and (3) assess whether existing anti-trust laws, competition policies, and current enforcement levels are adequate to address these issues”. The Subcommittee came up with a list of recommendations to regulate big techs (Amazon, Apple, Facebook and Google) in order to help reduce anti-competitive behaviour (US House (2020)).

<sup>40</sup> See EU Commission proposals of an EU Digital Markets Act (EC (2020b)) and an EU Digital Service Act (EC (2020c)).

## Recent changes in the competition framework for internet companies in China

On 10 November 2020, the State Administration for Market Regulation (SAMR) published for consultation draft guidelines on how antitrust measures should be applied to internet companies (including big techs). With the publication of the guidelines, SAMR seeks to prevent monopolistic behaviour of internet platforms, promote fair market competition and safeguard the interest of consumers.

The guidelines, which were proposed in accordance with China's Anti-Monopoly Law of 2008 and describe anti-competitive practices in the internet sector, cover the following key elements:

- **Exclusivity clauses.** Vendors should be able to sell their products on multiple platforms at the same time and not be forced to choose between internet companies.<sup>①</sup> Under current market practice, merchants are often asked to stick with one platform, a practice referred to as "pick one of two".<sup>②</sup>
- **Price discrimination based on customer data analytics.** The draft guidelines clarify how internet companies may price their offerings and how they may subsidise prices to attract new consumers. Subsidies that, for example, deter competition would be disallowed. Under current practice, customers are often quoted different prices generated by algorithms that use customers' online behaviour as inputs (eg spending behaviour, payment ability, consumption preferences and usage habits); and may face inflated prices or receive different levels of subsidies (sometimes taking prices below cost).
- **Market barriers.** Internet companies should not abuse their market power by erecting barriers around their ecosystems to keep competitors out. Under current practice, there is limited interoperability between big tech platforms; and users of one platform are often not able to access another platform's services without switching to the ecosystem of that platform.
- **Merger control.** The draft guidelines clarify that companies structured as Variable Interest Entities (VIEs), the prevailing structure for big techs, are obliged to submit potential acquisitions for antitrust review and seek permission from SAMR under China's Anti-Monopoly Law.
- **Review system.** The guidelines propose setting up a review system to ensure that internet companies do not abuse their market dominance. Consequences for violations may include requests for divestment of assets such as technologies or intellectual property; and modifications of algorithms.

Other recent changes in the regulatory environment for internet companies include draft rules for online lending which would require an internet company to fund 30% of the value of the loans it distributes (thereby limiting the funding provided by banks and other firms to 70%); and a draft law on personal data protection.

<sup>①</sup> A case in point are restaurants which should be able to sell through more than one delivery app. <sup>②</sup> For example, the two prominent e-commerce platforms in competition are Alibaba and Pinduoduo (Tencent); competing delivery apps are Ele.me (Alibaba) and Meituan (Tencent).

Sources: State Council of the People's Republic of China; Al Jazeera; *The Economist*; *Financial Times*; *Nikkei Asia*; Reuters; *The Wall Street Journal*.

These specific rules for big techs could include obligations for interoperability, limits on the bundling of services, prohibition of admission criteria leading to unfair discrimination against interested vendors, and constraints (or even bans) on the sale of their own products on the platforms they own.

Yet the most important – and most complex – issues are those related to the use of data obtained by big techs in their various activities. This comprehensive data availability constitutes a source of competitive advantage over other players (such as banks) in the market for specific financial services.<sup>41</sup>

An extreme way to address the potential for abuse of market dominance generated by data superiority is to restrict the use of data by big techs.<sup>42</sup> This approach would score well in terms of delivering a high standard on data privacy.<sup>43</sup> Yet it is also bound to create inefficiencies that may ultimately harm consumers.

A more promising approach is to facilitate data portability across all types of financial service provider as a way to avoid data monopolies. This is the rationale of open banking regulation that has now been adopted by an increasing number of jurisdictions.<sup>44</sup> That regulation obliges account service providers (such as banks) to share transaction data – upon clients’ consent – with other providers of payment services and to use, for that purpose, an efficient transmission technology (such as application programming interfaces (APIs)). This approach helps facilitate new entrants in the market. However, to date, the new provisions have been fairly asymmetric, as there are no equivalent rules that facilitate the transmission of big tech users’ data to other platforms or competitors (Fernández de Lis and Urbiola (2019)).

The European Union took a step towards solving this asymmetry with the General Data Protection Regulation (GDPR). GDPR establishes the principle (non-existent in other jurisdictions)<sup>45</sup> of users’ data ownership. GDPR requires all firms (controllers, in EU terminology) to share clients’ data with third parties at the customers’ request.<sup>46</sup> It also creates structures for European national data protection authorities to cooperate. Yet GDPR applies only to the data of natural persons and, unlike open banking regulations, does not contain a technical standard for the transmission of information that would guarantee its efficient use by the recipient. The development of the recent European Commission proposal for an EU digital markets act (EC (2020b)) provides an opportunity to fill those gaps.

Therefore, current data regulations fall short of ensuring a level playing field regarding access to users’ personal information, which could be relevant to the efficient provision of financial services by both banks and non-bank competitors. Specific entity-based rules on data-sharing obligations for big techs – following strict owners’ consent – could help address this possible market failure, thereby contributing to competition without an obvious adverse impact on other important policy goals.

## Section 5. Conclusions

Helping to achieve a level playing field in the provision of financial services is a desired outcome of the regulatory framework. This entails facilitating an orderly entry of new participants – such as fintechs and

<sup>41</sup> One example is the use of information on transactions in an e-commerce platform for the credit underwriting business. See Frost et al (2019).

<sup>42</sup> One example is the ruling by the German Federal Cartel Office, which in February 2019 prohibited Facebook from making use of customer data obtained from a specific service when offering a different one.

<sup>43</sup> See BIS (2019) for a comprehensive discussion of the trade-offs faced by authorities when designing data and competition policies.

<sup>44</sup> Examples are Australia, the European Union, Mexico and the United Kingdom.

<sup>45</sup> While there is no federal equivalent to GDPR in the United States, the California Consumer Privacy Act passed in early 2020 contains provisions similar to those of GDPR. Other states such as Illinois, Nebraska, New Hampshire, New York and Virginia are currently working on possible legislative reforms along the same lines.

<sup>46</sup> GDPR contains, however, the following provision: “The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format” (Article 20.1). Yet this falls short of requiring an API-like interface. Moreover, “the right to have the personal data transmitted directly from one controller to another” can only be exercised “where technically feasible” (Article 20.2).

big techs – that could expand consumers’ opportunity set, promote innovation and foster competition. However, it also requires unwarranted discrepancies in regulatory obligations to be avoided that might jeopardise the competitive position of incumbents (such as banks) vis-à-vis that of new entrants.

Yet fostering a level playing field is not the primary objective of financial regulation. Public policy goals such as financial stability, market integrity and consumer protection rank first in the order of priorities. Moreover, equating the conditions to be satisfied by different types of player in particular market segments would not always promote more competitive markets. Therefore, achieving a level playing field would only be desirable if higher-priority policy objectives are ensured.

In some policy domains, such as consumer protection or AML/CFT, an activity-based approach may well be adequate enough to achieve primary objectives. Yet in others, such as financial stability, an entity-based approach is indispensable. In a third group of policies, such as those on operational resilience and competition, regulations require a combination of activity- and entity-based rules, addressing the specific risks that different types of players can generate to meet those policy objectives.

Therefore, regulation may create unwarranted competitive distortions in two ways: first, by introducing specific entity-based obligations for a specific set of competitors on policy areas in which an activity-based approach could deliver the desired objectives; and second, by imposing specific obligations on some but not all types of players for which entity-based rules would be warranted on higher-priority policy grounds.

The existing regulatory framework in major jurisdictions does tend to impose comparable rules for consumer protections and AML/CFT on all relevant providers of financial services. Yet supervision and enforcement of these rules may be different across different types of entities that provide the same services. A functional – as opposed to a sectoral – organisation of financial supervision may help eliminate those unwarranted discrepancies and contribute to a more level playing field. In the area of AML/CFT, heightened vigilance of new, non-bank players’ activity seems essential in order to address current challenges in ensuring market integrity, as well as to mitigate distortions created by differences in the effective regulatory burden experienced by different types of entity.

The situation is different in policy areas for which entity-based rules may be appropriate. Despite recent progress, rules aimed at ensuring the adequate operational resilience of traditional financial institutions – such as banks and insurance companies – are generally more stringent than those for other entities. As things move forward, and some big techs continue to increase their presence in the financial services market, their operations may acquire systemic importance. This should be acknowledged by the regulatory framework. A complication is that they operate across a range of financial and non-financial business lines, thus requiring cooperation across different authorities.

Finally, with regard to competition, the potential of big techs to achieve a dominant position and to use that position to adopt anti-competitive practices may deserve specific action. An entity-based regulation targeting those risks, including rules that facilitate comprehensive and efficient data-sharing, seems a promising strategy.

In summary, there is currently only limited scope for further harmonising the formal requirements to be satisfied by different players in specific market segments without jeopardising higher-priority policy goals. In fact, contrary to what industry and other observers often claim, there seems to be a strong case for relying more, and not less, on entity-based rules. The current framework could be complemented with specific requirements for big techs that would address risks stemming from the different activities they perform. That strategy would not only improve the ability of financial regulation to achieve primary objectives, but would also help promote a level playing field. The concrete definition and the enforcement of those new rules would entail close cooperation across financial, competition and data protection authorities worldwide.

## References

- Arner, D, R Auer and J Frost (2020): "Stablecoins: risks, potential and regulation", *BIS Working Papers*, no 905, November.
- Association of Certified Anti-Money Laundering Specialists (ACAMS) (2019): "Fintech: friend or foe to anti-financial crime", June.
- Bank for International Settlements (BIS) (2019): "Big tech in finance: opportunities and risks", *Annual Economic Report 2019*, Chapter III, June.
- Bank of England, Prudential Regulatory Authority and Financial Conduct Authority (2019): *Building operational resilience: impact tolerances for important business services*, December.
- Basel Committee on Banking Supervision (BCBS) (2011): Principles for sound management of operational risk, June.
- (2016a): Sound management of risks related to money laundering and financing of terrorism, February.
- (2016b): Guidance on the application of the Core Principles for Effective Banking Supervision to the regulation and supervision of institutions relevant to financial inclusion, September.
- (2017): Guidelines for identification and management of step-in risk, October.
- (2018): Sound practices: implications of fintech developments for banks and banks' supervisors, February.
- (2020a): Sound management of risks related to money laundering and financing of terrorism: revisions to supervisory cooperation, July.
- (2020b): Consultative Document: revisions to the principles for sound management of operational risk, August.
- Blank Rome (2018): "The fintech revolution: complying with anti-money laundering laws to avoid regulatory enforcement actions", *White Collar Watch*, no 1, April.
- Calvo, D, J C Crisanto, S Hohl and O Pascual Gutiérrez (2018): "Financial supervisory architecture: what has changed after the crisis?", *FSI Insights on policy implementation*, no 8, April.
- Carstens, A (2018): "Big tech in finance and new challenges for public policy", keynote address at the FT Banking Summit, London, 4 December.
- (2019): "Data, technology and policy coordination", keynote speech at the 55th SEACEN Governors' Conference and High-Level Seminar, Singapore, 14 November.
- Cornelli, G, J Frost, L Gambacorta, R Rau, R Wardrop and T Ziegler (2020): "Fintech and big tech credit: a new database", *BIS Working Papers*, no 887 (also published as *CEPR Discussion Papers*, no 15357).
- Crémer, J, Y-A de Montjoye and H Schweitzer (2019): *Competition policy for the digital era*, European Commission.
- Crisanto, J C, J Ehrentraud and M Fabian (2021): "Big techs in finance: regulatory approaches and policy options", *FSI Briefs*, forthcoming.
- De la Mano, M and A Jorge Padilla (2018): *BigTech in finance*, December.
- European Commission (EC) (2013): *Competition law rules applicable to antitrust enforcement, volume III: sector specific rules situation*, July.

——— (2019): *Digital operational resilience framework for financial services: making the EU financial sector more secure*, December.

——— (2020a): “Digital Finance Strategy, legislative proposals on crypto-assets and digital operational resilience, Retail Payments Strategy”, Q&A, September.

——— (2020b): *Proposal for a Regulation of the Council and the European Parliament on contestable and fair markets in the digital sector (Digital Markets Act)*, December.

——— (2020c): *Proposal for a Regulation of the Council and the European Parliament on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC*, December.

Federal Financial Institutions Examination Council (FFIEC) (2019): *Business continuity management booklet*, November.

Financial Action Task Force (FATF) (2020): *FATF report to G20 on so-called stablecoins*, July.

Financial Stability Board (FSB) (2017): *Financial stability implications from FinTech*, June.

——— (2018): Cyber Lexicon definition of cyber security, November.

——— (2019): *BigTech in finance: market developments and potential financial stability implications*, November.

Financial Stability Oversight Council (FSOC) (2013): “Basis of the Financial Stability Oversight Council’s final determination regarding General Electric Capital Corporation”, July.

Fernández de Lis, S and P Urbiola (2020): *“Digital transformation and competition in the financial sector”*, BBVA Research, January.

Fratto, F and L Reiners (2019): “A new source of systemic risk: cloud service providers”, *The Finreg Blog*, August.

Frost, J, L Gambacorta, Y Huang, H S Shin and P Zaiden (2019): *“Big tech and the changing structure of financial intermediation”*; *Economic Policy*, vol 34, no 100, pp 761–99.

Institute of International Finance (IIF) (2017): Response to BCBS consultation on *Implications of fintech developments for banks and bank supervisors*.

——— (2019): *Cloud computing in the financial sector, part 3: cloud service providers (CSP)*, February

International Organization of Securities Commissions (IOSCO) (2020): *Principles on outsourcing*, May.

Joint Forum (BCBS, IOSCO, IAIS) (2005): *Outsourcing in financial services*, February.

——— (2006): *High-level principles for business continuity*, August.

Kirakul, S, J Yong and R Zamil (2021): “Multiple mandates”, *FSI Insights on policy implementation*, forthcoming.

Monetary Authority of Singapore (2020): “Ensuring safe management and operational resilience of the financial sector”, April.

Office of the Comptroller of the Currency (OCC) (2013): “Third-party relationships: risk management guidance,” *OCC Bulletin*, 2013-29, October.

Organisation for Economic Co-operation and Development (OECD) (2005): *OECD guiding principles for regulatory quality and performance*.

——— (2011): *Competition issues in the financial sector*.

People’s Bank of China (PBC) (2020): *“Financial regulators to have a regulatory talk with Ant Group”*, press release, 27 December.

Petralia, K, T Philippon, T Rice and N Véron (2019): "Banking disrupted. Financial intermediation in an era of transformational technology", *General Report on the World Economy*, CEPR.

Porter, K and N Velázquez (2020): Letter to US Treasury Secretary S Mnuchin.

Restoy, F (2019): "Regulating fintech: what is going on and where are the challenges?", speech at the ASBA-BID-FELABAN XVI Banking public-private sector regional policy dialogue on *Challenges and opportunities in the new financial ecosystem*, Washington DC, 16 October.

Stone, T (2016): "Fintech: the emerging financial crime compliance minefield", May.

Thomson Reuters Legal (2018): "Five best fintech compliance and regulatory practices for financial professionals".

US House of Representatives (US House) (2020): "Investigation of competition in digital markets", *Majority staff report and recommendations*, House Judiciary Committee's Subcommittee on Antitrust, Commercial and Administrative Law, October.

Vives, X (2016): *Competition and stability in banking: the role of competition policy and regulation*, Princeton University Press.