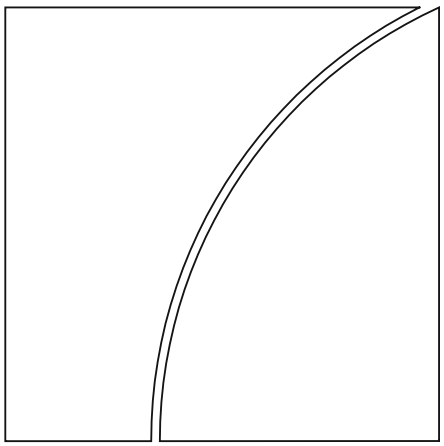
Financial Stability Institute

FSI Insights

on policy implementation

No 60



A two-sided affair: banks and tech firms in banking

By Irina Barakova, Johannes Ehrentraud and Lindsey Leposke

October 2024

JEL classification: G18, G21, G23, G28, L41, L51
Keywords: Tech firms, fintechs, big techs, banking, partnerships, banking-as-a-service, deposits, credit, payments, regulation, consolidated supervision, conglomerate supervision, financial stability

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees, the Office of the Comptroller of the Currency (OCC), the Department of the Treasury, or the United States government.

Authorised by the Chair of the FSI, Fernando Restoy.

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

ISSN 2522-249X (online)
ISBN 978-92-9259-796-2 (online)

Contents

A two-sided affair: banks and tech firms in banking[1]

Executive summary

The widespread adoption of digital technology is fundamentally altering the way customers interact with the financial system. Digital advancements have opened avenues for tech firms to broaden their presence in the financial sector, stimulating demand for innovative methods of payment, borrowing and saving. Today, with just a few taps on a mobile device, access to banking services can be executed swiftly and seamlessly, often without a bank in sight from the customer's perspective.

Tech firms, including big techs and fintechs, have come to deliver various financial services that are typically provided by banks. These services allow users to access payment, credit or depository services ("banking services"). They primarily cater to consumers and small businesses and often feature unique functionalities due to their distinct access points, setting them apart from those offered by traditional banks.

Tech firms generally obtain a licence or form partnerships with banks to deliver banking services. Observations from a sample of big techs and large fintechs suggest that a given firm typically uses a mix of both, which may be related to its motivation for providing specific banking services, the availability of options at the jurisdictional level, and the disparities in requirements for licences and partnerships.

Tech firms have traditionally provided banks with back-end services, but now they are also entering front-end partnerships with banks. In back-end partnerships, a non-bank provides technology services to a bank, such as cloud computing. Meanwhile, in front-end partnership arrangements, the bank provides its infrastructure (such as the ability to access the payment systems) to operationalise the non-bank's offering of financial services, while the non-bank engages directly with the customer.

Big techs' offering of depository products through bank partnerships has been relatively limited so far, with deposit-taking partnerships more commonly found between fintechs and banks. In deposit-taking partnerships, tech firms facilitate the delivery of depository products directly to their customers via digital platforms. Although the tech firm typically manages the customer interface, the deposit itself is held on the bank's balance sheet.

There are numerous instances of lending partnerships between banks and tech firms. In a direct lending partnership, borrowers can access credit through a tech firm's digital platform, with banks and tech firms taking on a variety of roles in the credit origination process. Another variant of a lending partnership is a credit referral arrangement where the tech firm acts as a broker to a bank, introducing eligible customers to specific lending products, often after conducting a pre-screening analysis.

The nature of payment partnerships is highly diverse. In order to provide payment-related services, tech firms frequently rely on payment infrastructures which are typically only accessible to banks. However, in some countries, non-bank entities, including tech firms, can directly access payment systems or even operate their own systems. Digital wallets are a prominent type of payment partnership.

The increasing involvement of tech firms in banking services has transformed the structure of value chains within the banking sector. Traditionally, the banking business model operates on an

[1] Irina Barakova, former Member of Secretariat, Basel Committee on Banking Supervision; Johannes Ehrentraud (johannes.ehrentraud@bis.org), Bank for International Settlements; and Lindsey Leposke (Lindsey.Leposke@occ.treas.gov), Office of the Comptroller of the Currency. We are grateful to Juan Carlos Crisanto, Elisabeth Noble and Monika Spudic for helpful comments. We also extend our appreciation to the authorities and banks who generously shared their perspectives during the interviews. Anna Henzmann provided valuable administrative support.

integrated, vertical value chain. However, the entry of tech firms, either through partnerships with banks or by obtaining monoline licences, has given rise to a new expanded and more distributed banking value chain. In this new value chain, banks are pushed further away from the customer relationship; however, they typically remain involved in at least one layer of the value chain.

While the expanded and more distributed value chain presents opportunities, it also poses challenges for banks and supervisors. This new approach could broaden consumer access to new markets and enhance efficiency by allowing firms to specialise in areas where they have a competitive edge. However, as more entities participate in delivering a single product or service, this can heighten prudential and conduct risks. Specifically, front-end partnership arrangements can introduce operational risks, compliance risks (including in relation to anti-money laundering and countering the financing of terrorism (AML/CFT)) and reputational risks, which may differ depending on the specific banking service provided. There may also be concerns around data privacy and security, consumer protection, large tech firms' negotiating power vis-à-vis banks and banks' business model sustainability. Additionally, as responsibilities and risks become dispersed among numerous entities within the value chain, the regulatory boundaries become increasingly blurred, posing novel challenges for day-to-day supervision.

In most jurisdictions, however, there are no direct regulatory restrictions for tech firms to partner with banks to provide banking services. By standard practice, regulators primarily manage potential risks from such partnerships by regulating and supervising the bank partners. The general principle is that banks' partnerships with third parties do not diminish their responsibility to ensure activities are performed in compliance with regulatory requirements. Thus, supervisory oversight over tech firms is typically indirect and limited.

In some jurisdictions, authorities have implemented a blend of measures to manage partnerships between tech firms and banks. These include initiatives to: (i) gather more information; (ii) adjust prudential/conduct requirements and/or clarify supervisory expectations in different policy areas, including operational resilience, financial soundness, consumer protection, AML/CFT and competition; and (iii) review the regulatory perimeter and supervisory approach.

Big techs present unique challenges in partnerships due to their size, negotiating power and banks' potential oversight limitations. If front-end partnerships become more prevalent, big techs' role in financial services could grow, necessitating careful monitoring of the multifaceted role big techs play, both as providers of financial services and as service providers to financial institutions. In addition, the emergence of new corporate structures may require specific entity-based rules for big tech operations in finance to address risks not covered by current frameworks.

Tech firms' growth and evolution in the banking sector has implications for the banking value chain that may warrant additional policy responses. The complexity of partnerships and expansion of tech firms, particularly big techs, in delivering banking services across multiple jurisdictions without consolidated oversight, limits visibility for regulators. Over time, if left unchecked, this could have significant implications for public trust, a fundamental pillar for the soundness of the banking system, and consequently financial stability. Therefore, additional actions at the national level, supported by international policy cooperation, could be warranted.

Section 1 – Introduction

1. **The business of banking is changing.** Less than 60 years ago, the banking industry saw the introduction of the automated teller machine (ATM), an innovation born out of consumers' frustration with limited banking hours.[2] This trend of innovation continued with the ubiquitous magnetic strip on plastic cards, which has now been largely replaced by smart cards and the convenience of smartphone payments.[3] Today, with just a few taps on a mobile device, consumers can initiate peer-to-peer (P2P) payments, make purchases through short-term credit extensions like buy now, pay later (BNPL) products, and even open new savings accounts via their mobile device app. All these banking services[4] can be executed swiftly and seamlessly, often without a bank in sight from the perspective of the consumer.

2. **The demand for digital financial services is fuelled by customer expectations and the availability of new technologies in a rapidly evolving digital landscape.** The widespread use of digital technology is fundamentally transforming customer interaction with financial institutions. Especially among younger generations, there is a growing demand for instantly available financial services that offer a user-friendly experience with minimal or no fees. This shift mirrors the trend of smartphones becoming the central hub for communication, and the increasing preference for mobile apps that consolidate a wide range of services (eg e-commerce, social networking, transportation, food delivery and banking) within a single platform.

3. **These developments have set the stage for tech firms to expand into banking.** By leveraging their technological advantage, tech firms[5] have been able to offer a wide range of financial services through digital channels. Moreover, they have created innovative methods of payment, borrowing and saving that are offered to consumers through new access points. By doing so, they attempt to provide a seamless and convenient banking experience to customers, and extend their reach to previously underserved segments, particularly in emerging market and developing economies (EMDEs) or in rural areas where operating physical branches would be economically unfeasible.[6]

4. **The involvement of tech firms in banking introduces benefits and risks.** The benefits encompass potential enhancements in market efficiency, financial inclusion and customer convenience.[7] Conversely, tech firms may create risks in different policy domains such as competition, data, conduct of business, operational resilience and financial stability.[8] The potential impacts of these risks may be accentuated for big techs and large fintechs. In a broader perspective, there are concerns that, within the current regulatory framework, safeguarding public trust in the banking sector may become increasingly challenging as non-banks, such as tech firms, provide or deliver banking services.

5. **While tech firms' provision of banking services has received growing attention, unresolved questions remain about their impact on the banking sector and the nature of partnership arrangements.** Several studies, including publications by standard-setting bodies, have assessed the potential future scenarios of tech firms' expansion into banking and the different roles incumbent banks

[2] Barclays (2017).

[3] FasterCapital (2024).

[4] For the purposes of this paper, we use the term "banking services" to describe financial services that are traditionally offered by banks or that are marketed as similar to financial services offered by banks. These banking services can also be provided by tech firms, granted they hold the appropriate bank or non-bank licences.

[5] Tech firms include both fintechs and big techs, as defined in Section 2.

[6] See Croxson et al (2022).

[7] See eg Beck et al (2022), Frost et al (2019), Gambacorta et al (2019, 2023) and Luohan Academy Report (2019).

[8] Crisanto, Ehrentraud, Lawson and Restoy (2021).

and tech firms may play.[9] For example, in 2018 the BCBS highlighted that the position of incumbent banks is likely to be challenged under a range of different scenarios, and that the future role of banks will increasingly involve a "battle for the customer relationship and customer data".[10] Moreover, in 2024 the BCBS elaborated on potential risks from digitalisation to banks, emphasising that new entrants partnering with banks, particularly big techs, have the potential to become dominant competitors.[11]

6. **The strategies tech firms use to provide banking services are increasingly complex and evolving.** Some hold their own bank or non-bank licences, where required, whereas others offer their services in partnership with financial institutions such as banks, and many use a combination of both. Moreover, the ongoing evolution and proliferation of front-end partnerships is creating greater interdependencies between banks and tech firms, blurring the boundaries between banking and non-financial activities, and replacing the primarily direct relationships in banking with long-intermediated chains of discrete services. As Acting Comptroller of the Currency Michael Hsu put it, "banking, in short, is beginning to resemble global manufacturing supply chains". He also warned that "paying insufficient heed to the growing complexity of arrangements between banks and nonbanks risks an increase in consumer harm, runs, and potential threats to monetary stability".[12]

7. **This paper reviews how tech firms provide banking services and assesses the potential policy implications.** It is intended to broaden and deepen understanding of: (i) the ways in which tech firms provide banking services, in particular in partnerships with banks, and regulatory approaches across jurisdictions; and (ii) the implications for the banking value chain and related risks.[13] It is based on interviews with nine regulatory bodies and seven banks from geographically diverse jurisdictions, together with a desktop review of public information and related regulations, and the authors' own analysis.[14]

8. **The remainder of this paper is structured as follows.** Section 2 provides an overview of tech firms' activities in banking services and examines the ways in which tech firms deliver banking services. Section 3 explores bank-tech partnerships in more detail. Section 4 focuses on implications for the banking value chain. Section 5 describes policy responses and offers policy considerations for financial authorities, and Section 6 concludes.

9 See BCBS (2018, 2019, 2024b,c)) and FSB (2019a,b)).

10 BCBS (2018).

11 The risks highlighted include strategic, reputational and operational risks, data issues and financial stability risks. See BCBS (2024).

12 Hsu (2024).

13 The banking service value chain represents the process for delivering products and services to customers and includes the customer relationship and required infrastructure to facilitate the delivery to consumers. See US Department of Treasury (2022).

14 The authors approached eight large tech firms for interviews. One declined; the others did not respond. All interviews were held under Chatham House rules; consequently, no information in this paper is attributed to a specific institution.

Section 2 – Tech firms' involvement in banking services

9. **This section explores the involvement of tech firms in banking services, examining three key aspects: who, what and how.** It outlines the types of tech firms under consideration and their motivation for offering banking services. Subsequently, it details the diverse banking services that tech firms provide and how these correspond to traditional banking services. Lastly, it explores the regulatory options for tech firms' entry into banking and describes observed cases among select tech firms. Although some tech firms also provide technology services to banks, the emphasis here is on their direct involvement in providing banking services and managing customer relationships.

Tech firms: from fintechs to big techs

10. **The universe of tech firms is vast, but we can broadly categorise them into two groups.** The first comprises tech firms whose core business focuses on using digital technology to deliver financial services either solely or primarily online.[15] This includes standalone fintechs, which tend to have a narrow business model as well as larger, diversified fintechs that provide a broader range of (mainly) financial services through various channels. The second category comprises big techs, defined by the Financial Stability Board (FSB) as large technology companies with extensive customer networks and includes firms with core businesses in social media, internet search, software, online retail and telecoms.[16]

11. **Big techs stand out among tech firms due to their unique "data-network-activities" (DNA) loop.** They differ from other tech firms given their unique business model and digital ecosystem that is interconnected and interdependent across numerous businesses and often geographic regions. By taking advantage of advanced technology to analyse vast amounts of data, big techs have the ability to create further user activity by offering new, or improving existing, products and services. The wider a big tech's offering, the more attractive its platform is for its users and the more data are generated. The result is a self-reinforcing ecosystem characterised by strong network effects where user growth expands both the data available to big techs and the services offered by them. Overall, the DNA loop affords big techs the ability to establish a substantial presence in new market segments quickly, including in the financial sector.[17]

12. **Big techs' motivation in offering banking services probably differs from that of fintechs or traditional banks.**[18] Fintechs and banks focus solely on financial services, while big techs' core businesses are primarily non-financial. Their foray into banking does not appear to be driven by an ambition to supplant banks, but rather to support their original business by enhancing the user experience within their digital platforms and to further reinforce their DNA loop. Also, by offering selected banking services, big techs can reap several benefits, including diversified revenue streams,[19] richer customer data[20] and expanded platform functionality. These benefits may also allow big techs to provide financial services more cost-effectively and derive indirect profits, for instance, by leveraging the financial data collected to

15 Zamil and Lawson (2022).

16 FSB (2020).

17 See BIS (2019), Crisanto, Ehrentraud and Fabian (2021), Croxson et al (2022), Feyen et al (2021) and Frost et al (2019).

18 See FSB (2019b) and Ehrentraud et al (2022).

19 For example, e-wallets have become a significant source of fee income.

20 Big techs may be drawn to the financial services sector due to the wealth of data it offers. Since big techs can monetise those data, they do not necessarily need to profit directly from the financial services they provide, which can give them a competitive edge in the market.

improve their non-financial product offerings and fostering increased customer dependence on their ecosystem.[21]

Types of banking services

13. **Tech firms may engage in different types of banking activities.** Their main banking activities encompass the three traditional services provided by banks:[22]

- **Deposits.** Tech firms may operate digital platforms that deliver depository services, such as demand deposits or time deposits, to consumers or businesses. This is often done through partnerships with banks, which allows these banks to access deposits from customers they might otherwise be unable to reach. Additionally, some tech firms have entities in their groups that have obtained a banking licence and are therefore allowed to take deposits.
- **Payments.** These include, among others, P2P payment services, which allow individuals to send money directly to each other; online payment processing services, which allow businesses to accept payments online; and digital wallets (also mobile or e-wallets[23]), which allow users to store and manage their credit and debit card information on their devices and make payments online or in-store.[24] In addition, tech firms may offer their customers the possibility to store value in payment/transaction accounts in the form of e-money.[25] These accounts closely mimic bank deposit accounts and customers may use them in lieu of bank deposits accounts while not being fully aware of their differences.[26]
- **Credit.** Tech firms, particularly big techs, often provide credit to retail customers or small and medium-sized enterprises (SMEs) on their e-commerce platforms. They may also offer BNPL services, which allow customers to purchase items and pay for them over time.[27]

14. **Banking services provided by or through tech firms may have unique features or functionalities, owing to their distinct access points, that set them apart from conventional banking.** Rather than replacing conventional banking services, tech firms are reshaping how these services are accessed and utilised. For example, they may design or offer products to meet the specific needs of customers on their platforms, which may not always align neatly with the traditional categorisation of banking activities.[28] While the primary customers of these services are consumers and small businesses operating on these platforms (eg merchants on e-commerce platforms), tech firms, specifically big techs,

[21] This motivation is more akin to "captive finance" where manufacturing firms support downstream firms. See Liu et al (2024).

[22] There is no standardised set of banking services. At the heart of banking, however, is the acceptance of deposits, which allows for financial intermediation and lending. Moreover, their well established access to payment systems enhances their ability to provide payment services.

[23] A digital wallet can be defined as a software application (usually running on a personal device or computer) that stores payment information and allows users to communicate with other enabled devices via non-financial company technology to complete transactions. See OCC (2021).

[24] Other services may include international money transfers or digital asset services related to facilitate payments (eg PayPal coins).

[25] E-money refers to debt-like instruments that an entity issues on receipt of funds for the purpose of facilitating payment transactions. See Box 1 in Ehrentraud et al (2021).

[26] For example, e-money accounts are typically not covered by deposit insurance schemes.

[27] In terms of volumes, research by Cornelli et al (2023) indicates that, despite variations at the country level, credit provided by tech firms reached around $800 billion in 2020. Out of this, big tech credit accounted for $700 billion, while the remaining $100 billion was attributed to fintech credit.

[28] An example of this could be accounts that are not traditional deposit accounts but are used for storing value in the form of e-money.

also facilitate connections between their customers and banks for traditional banking products like credit cards, collateralised loans and wealth management.

Regulatory options

15. **The main ways to provide banking services are holding a licence or entering into partnerships with banks.** In principle, tech firms' financial operations are subject to the same requirements as those of other financial market participants offering similar products.[29] If a tech firm chooses to operate through its own licence without a bank as partner, it must adhere to the requirements associated with that licence. Alternatively, if it opts for a partnership, the tech firm is indirectly affected by the requirements imposed on its bank partner (Figure 1).[30] These options allow tech firms to offer banking services that may be in competition or in partnership with banks, or both at the same time.

Tech firms' entrance into banking services — Figure 1

Source: Authors' conceptualisation.

16. **Regulatory frameworks may restrict tech firms' options in terms of how they provide banking services.** For example, in the United States there is a long-standing policy of separating commerce and finance, barring non-financial companies (NFCs) from operating banks.[31] While monoline licences are commonly available to tech firms for lending and payments, they are not for deposit-taking, consistent with the expectation that deposit-taking is primarily reserved for entities that are licensed and regulated as banks.[32] As for partnerships with banks, tech firms typically face no direct restrictions in delivering payment and lending services, though certain countries, such as China, do not allow partnerships for taking deposits (Table 1).

[29] See Crisanto, Ehrentraud and Fabian (2021).

[30] While not a focus of this paper, big techs may also be entering banking services by partnering with fintech firms or acquiring them. For example, Amazon and Affirm have partnered to provide BNPL, Tencent and Flywire have partnered to provide payment services, and Meta and Indifi have partnered to provide credit services.

[31] Except state-sponsored industrial loan charters (ILCs), which are available only in a few states. See Box B in FSB (2019).

[32] According to Basel Core Principle 4, the act of accepting deposits from the public is limited to institutions that hold a banking licence and are subject to supervision as banks. The principle also highlights that in certain countries, non-banking financial institutions that accept deposits may be subject to different regulations compared with banks; and that these institutions should be subject to a regulatory framework that is appropriate for the nature and scale of their operations (BCBS (2024d)). Against this backdrop, some jurisdictions allow certain non-bank entities to accept term deposits (Ehrentraud et al (2024)).

Regulatory approaches: permissible ways for tech firms to provide financial services Table 1

Jurisdiction	Bank partnership			Monoline licence			Banking licence
	Deposits	Payments	Lending	Deposits[1]	Payments[2]	Lending	
Brazil	✓	✓	✓	✗	✓	✓	✓
China[3]	✗	✓	✓	✗	✓	✓	✓
Hong Kong SAR	✓	✓	✓	✗	✓	✓	✓
India[4]	✓	✓	✓	✗	✓	✓	✓
Singapore	✓	✓	✓	✗	✓	✓	✓[5]
European Union	✓	✓	✓	✗	✓	✓	✓
United Kingdom	✓	✓	✓	✗	✓	✓	✓
United States	✓	✓	✓	✗	✓	✓	✗[6]

[1] The column indicates where monoline licences are available for taking demand deposits. In some countries, non-bank financial institutions (NBFIs) are allowed to accept deposits other than demand deposits. [2] For the purposes of this paper, a payment monoline licence includes a payment institution and e-money institution licence in the EU and UK, an instituição de pagamento in Brazil, a money service business licence in the US and a stored value facility provider licence in China. [3] Regulations in China prevent tech firms from holding more than 30% in a digital bank, essentially preventing them from having a controlling stake. China banned banks from online deposit-taking through third-party online platforms. [4] Monoline licences available in India provide for different restricted activities which can be undertaken by licenced entities, including accepting time deposits, lending and payments. [5] In 2020, the Monetary Authority of Singapore (MAS) awarded four digital bank licences, which allowed entities without a track record in banking to conduct digital banking businesses in Singapore. These entities were either wholly owned by or part of consortia comprising tech firms. MAS is currently not granting new digital bank licenses. [6] In the US there is a historical separation of banking and commerce, which may limit some tech firms, particularly big techs, from obtaining a banking charter. The exception are industrial loan companies. These licences are available in only a few states.

Sources: FSI analysis.

17. **Even where tech firms have multiple options, authorities may have differing views on the potential challenges they involve.** Based on the interviews conducted for this paper, some authorities emphasise the advantages of tech firms providing banking services through their own bank licence, which allows for direct oversight and access to information. Others stressed the merits of partnerships, which retain incumbent banks as the main addressees of regulatory actions while enabling them to leverage tech interfaces, a capability they may lack the resources or skills to develop internally.

Bank licences

18. **While obtaining a banking licence entails stricter regulatory oversight, it also offers a range of advantages.** A banking licence bolsters public trust and legitimacy, potentially allowing tech firms to scale up more easily in financial services. It also allows them to bundle services along the value chain, complementing their existing product offerings without the need to involve third-party banks.[33] Furthermore, it grants access to deposits as a low-cost source of funding which may be particularly relevant for fintechs. However, holding a banking licence also means being subject to comprehensive regulation by prudential authorities, which also have the legal authority to gather

[33] Conversely, a banking licence may restrict its holders from engaging in certain activities.

information to assess risks that may affect the bank, as well as enforcement powers within the banking regulatory perimeter.[34]

19. **Despite historical concerns regarding the ownership of banks by NFCs, several banking authorities have allowed tech firms to own banks.** As pointed out by Zamil and Lawson (2022), prudential authorities have traditionally discouraged such affiliations based on four main concerns: (i) the potential increase in conflicts of interest; (ii) the erosion of competition leading to a concentration of power; (iii) heightened systemic risk and contagion; and (iv) the hindrance to effective consolidated supervision. Despite these concerns, several jurisdictions now allow NFCs to own banks, though they may impose a range of additional requirements on them. One example is the imposition of a financial holding company (FHC) structure. This structure is designed to encapsulate the diverse financial activities of tech firms, thereby facilitating consolidated oversight (eg China and the EU).[35]

20. **Where tech firms operate a bank, it is often licensed under regulatory frameworks for digital-only banks.** In the jurisdictions that have set specific regulatory frameworks for banks that exclusively deliver banking services through digital channels, the main licensing and ongoing requirements are similar to those for traditional banks. However, digital banks face restrictions on their physical presence and, in some cases, the market segments they are allowed to serve. They also face more stringent requirements on technology-related elements.[36] Importantly, their requirements on ownership and control may be more permissible towards NFCs than those applicable to other banks. This may be one reason, in addition to tech firms' digital business model, why digital bank licences are typically sought by tech firms, where available.

Monoline licences

21. **Tech firms may conduct financial activities through monoline licences, which are specific to a particular financial service.** For instance, a payment licence allows the provision of payment services, while a non-bank lending licence enables the offering of credit services. As such, a tech firm may have several subsidiaries in its group with different monoline licences in numerous countries.

22. **Monoline licences offer an alternative to banking licences for tech firms.** While a monoline licence enables a tech firm to provide services that may complement its other product offerings, it avoids some of the substantial compliance costs associated with running a bank. In addition, it is less costly to obtain and subject to less demanding regulatory requirements than a banking licence. These requirements typically apply at the level of the individual legal entity and not to other entities within the same group on a consolidated basis. Also, even where banks and monoline licence holders face the same requirements, they may be subject to different levels of supervision over their business practices.

23. **Monoline licences are available in most jurisdictions for lending or payment services but not deposit-taking.** In many jurisdictions, monoline licences allow non-banks to offer retail credit products such as consumer or business loans, or payment services such as accepting, managing or transferring customer funds and/or store of value services (eg operating e-money accounts).[37] However, they are typically not available for deposit-taking (Box 1).

[34] Prudential requirements under the Basel Framework apply to internationally active banks on a consolidated basis up to the level of the bank's parent holding company. The scope of application of the Basel Framework includes "on a fully consolidated basis, any holding company that is the parent entity within a banking group to ensure that it captures the risk of the whole banking group" (SCO10.2).

[35] See Annex 2 in Ehrentraud et al (2022).

[36] For example, fit and proper requirements tend to be more prescriptive in relation to board members' expertise in technology and a satisfactory track record in operating a technology business may be required. See Ehrentraud et al (2020).

[37] For example, in India, non-bank payment aggregators – entities that help merchants connect with acquirers – are allowed to receive payments from customers, pool and transfer them on to the merchants once authorised by the RBI. See RBI (2020).

Box 1

Regulatory requirements for monoline licences

Requirements for monoline licences vary across jurisdictions and depend on the service provided (ie deposit-taking, payment services and/or lending).

Deposit-taking is banks' core activity, and it usually requires a banking licence, often alongside lending. However, in some jurisdictions a monoline licence for retail lending permits holders to accept term deposits from the public, with certain restrictions. In jurisdictions where NBFIs can take deposits, they are typically restricted from offering current accounts or demand deposits and generally face stricter requirements than other NBFI lenders that rely on other sources of funding.①

Payment services are typically subject to licensing and other requirements. In most jurisdictions, non-banks – including tech firms – are allowed to provide payment services or issue e-money.② These services may require different licences which may depend on the specific type of service provided, the transaction volume or value, and the geographic areas covered by the service. Some requirements, while imposed across payment services, may be applied differently. This is the case for licensing/registration requirements, minimum capital, safeguarding funds and other security requirements, and interoperability. Other requirements are in general uniformly applied across payment services, such as those relating to risk management, including AML/CFT, cyber security, data protection and consumer protection.③

Entities that engage in retail lending, including tech firms, are subject to a patchwork of regulatory rules. Regulatory approaches range from extending all or some aspects of the prudential framework for banks to non-bank lenders, to focusing mainly on the conduct of business and consumer protection. Licensing requirements also vary considerably across countries. For example, in some countries multiple licences may be required to engage in the full set of lending activities, whereas in others, a single licence suffices. In others, certain types of credit may be unregulated or require registration with a relevant authority (eg for AML/CFT purposes).④

① See Ehrentraud et al (2024). ② In some jurisdictions (eg South Africa), only banks are allowed to issue e-money. ③ See Ehrentraud et al (2021). ④ See Ehrentraud et al (2024).

24. **Brokering activities related to connecting a customer with a bank's services may also require a monoline licence.** Where this is the case, even if a tech company does not directly handle money, it might still need a licence depending on how it interacts with a partner bank. For example, in the UK, if a tech firm is introducing customers or certain businesses[38] to third-party finance providers such as banks, it needs to be authorised as a credit broker by the Financial Conduct Authority (FCA).[39] In the EU, brokers of consumer or mortgage credit are subject to requirements under the Consumer Credit Directive (CCD) and Mortgage Credit Directive (MCD).[40] In addition, entities providing payment initiation services in the EU, which involve initiating a payment order at the payer's request with respect to a payment

[38] This includes businesses that meet the FCA's definition of an individual, defined as: a sole trader, a partnership of two or three people not all of whom are bodies corporate, or an unincorporated body of people which does not consist entirely of bodies corporate and is not a partnership (FCA (2023b)).

[39] Credit brokers as defined by FCA (2023b) include: (i) primary credit brokers whose main business is helping customers find credit and hire agreements; and (ii) commercial brokers who help unincorporated firms, sole traders and small partnerships find credit.

[40] Different rules may apply to the brokering of deposits. For example, in Austria the brokering of deposits or certain other transactions is designated as "banking business" pursuant to the Banking Act and requires a bank licence (except for transactions conducted by contract insurance undertakings). See Austrian Banking Act (BWG), Article 1 para 1 Z 18.

account held at another payment service provider, need to be licensed as a payment or e-money institution.[41]

Partnerships

25. **Tech firms may enter into partnerships with banks to give their customers access to banking services, such as deposit, credit or payment services.** These so-called front-end partnerships, in which tech firms serve as the customer-facing delivery channel, offer a viable alternative for them to provide banking services without obtaining a licence and being subject to the regulatory requirements that come with it. There are also other types of partnership arrangements in which the tech firm provides technology services to financial institutions. While these are not the primary focus of this paper, both types are discussed in Section 3.

26. **By standard practice, regulators primarily manage potential risks from partnerships by regulating and supervising the bank partners.** The general principle is that banks' partnerships with third parties do not diminish their responsibility to ensure activities are performed in compliance with regulatory requirements, including when a third party delivers banking products or conducts risk management functions on behalf of the bank.[42] For example, banks are already subject to conduct of business requirements and obligations designed to ensure they can effectively withstand and recover from severe operational risk-related events. Nevertheless, regulators may discourage or limit certain partnerships to mitigate related risks.

27. **In most jurisdictions, there are no direct restrictions on tech firms partnering with banks to provide banking services.** The exception in some countries is deposit-taking partnerships. In China, for example, banks are not allowed to take deposits through third-party online platforms.[43] When it was allowed, for some Chinese banks up to 70% of their deposits came through such platforms. In India, for bank deposits mobilised by tech firms' services, customers have the option to access their accounts directly through the bank or through the tech firm's digital platform.

Range of observed activities

28. **Tech firms offer banking services through a combination of licences and partnerships.** Looking at a sample of seven big techs and two large fintechs in the Americas, Asia and Europe, tech firms' entry and offerings vary. All nine firms engage in payments and lending services across jurisdictions, and some also provide deposit services. Table 2 gives an overview of the approaches taken.

- **Banking licence.** Out of the nine tech firms, three have fully or majority-owned entities in their group that hold banking licences in the European Union or Hong Kong SAR.[44] In China, two hold minority stakes in entities with banking licences.[45]

[41] Payment initiation service providers help consumers to make online credit transfers and inform the merchant immediately of the payment initiation, allowing for the immediate dispatch of goods or immediate access to services purchased online. As such, they constitute an alternative to credit card payments for making online payments. See European Commission (2018). For example, one of Google's subsidiary companies is authorised as e-money institution in Lithuania and licenced to provide payment initiation and account information services. See EUCLID - Register (europa.eu). However, tech firms that only operate digital wallets do not require a payment licence. For example, Apple is not required to hold a payment licence to offer Apple Pay to customers in the EU. See European Commission (2021).

[42] BCBS (2024c).

[43] General Office of the China Banking and Insurance Regulatory Commission Circular of the General office of the People's Bank of China on Regulating Commercial Banks' Personal Deposit Business through the Internet.

[44] EU: PayPal (Europe)/PayPal; Hong Kong SAR: Ant Bank (Hong Kong)/Ant Group and Fusion Bank/Tencent.

[45] MYbank/Ant Group (30%), WeBank/Tencent (30%).

- **Monoline licences.** All nine tech firms have entities in their groups that hold payment licences, allowing them to provide payment services and/or issue e-money. While some firms also have licences for granting credit, monoline licences for deposit-taking are less common.
- **Partnerships with banks.** A majority of the selected tech firms collaborate with banks for granting credit and offering payment-related services such as digital wallet services. However, very few big techs use partnerships for deposit-taking services.

29. **Based on this sample, it appears tech firms employ a mixed strategy to offer or deliver banking services.** Entry through a banking licence is limited and primarily observed in Asia. Monoline licences and partnerships are commonly used for payments and lending.

Tech firm approaches to entry in selected jurisdictions Table 2

Tech firms	BT/LFT[1]	Bank partnership[2]			Monoline licence			Banking licence
		Deposits	Payments*	Lending	Deposits	Payments[3]	Lending	
Apple	BT	US	Global**	×	×	UK, US	UK,[8] US	×
Amazon	BT	×	×	EU, IN, US	×	EU, IN, UK, US	UK,[8] US	×
Ant Group	BT	×	×	CN	×	CN, EU, HK, SG, UK,[7] US	CN, UK[8]	CN,[4] HK, SG
Google	BT	×	Global**	IN	×	BR, EU, IN, UK, US	×	×
PayPal	LFT	US	Global**	IN, US	×	BR, HK, SG, UK, US	×	EU
Mercado Libre	BT	×	×	×	×	AR, BR,[5] CL, MX, PE, UY	AR, BR, CL, MX	×
Meta	BT	×	IN	IN	×	BR, EU, US	×	×
Nubank	LFT	×	×	×	MX[6]	BR[5]	BR, MX	×
Tencent	BT	×	×	CN	×	CN, EU	×	CN,[4] HK

[1] BT= big tech; LFT= large fintech. [2] These columns reflect front-end partnerships with banks (they do not include tech firms' partnerships with each other). [3] For the purposes of this paper, a payment monoline licence includes a payment institution and e-money payment institution license in the EU and UK, an instituição de pagamento in Brazil, a money service business licence in the United States and a stored value facility provider in Asia. [4] Regulations in China prevent tech firms from holding more than 30% in a digital bank. All "parents" of Chinese digital banks have stakes at or around this amount. [5] In Brazil, Mercado Libre and Nubank are considered prudential conglomerates and subject to prudential requirements. See Box 4 for additional detail. [6] Nubank has a Sociedades Financieras Populares (SOFIPO) licence in Mexico which allows the tech firm to take deposits. In October 2023, Nubank applied for a banking licence in Mexico. [7] Alipay (UK) Limited has been authorised as an e-money institution since February 2021. See Alipay (UK) Limited (fca.org.uk). [8] Authorised as a credit broker. Credit brokering is a consumer credit permission which does not allow a firm to lend. See www.fca.org.uk/firms/authorisation/consumer-credit-brokers/primary-credit-brokers.

(*) This table does not include arrangements between banks and tech firms related to card issuances such as credit or debit cards (eg co-branded credit cards) due to these types of arrangements being widely recognised and common across industries, such as tech firms, hotels, airlines etc.

(**) Digital wallets.

Sources: Company regulatory filings; supervisory licensing registries, FSI analysis.

30. **The availability of options at the jurisdictional level and the disparities in requirements for licences and partnerships may influence tech firms' choices between licences and partnerships.** Payments, for example, one of the earliest financial services provided by big techs, is an activity which tech firms have pursued with both partnerships and monoline licences. Specifically, in the EU many big techs hold an electronic (e-)money licence, such as Amazon and Ant Group. However, some big techs provide payment services through partnerships with licensed entities, thus operating without a payment licence in

the EU (eg Apple Pay).[46] Additionally, some tech firms (eg Amazon) maintain partnerships even if they could provide some of the partnership services, like credit card issuance, under their existing licences.[47] The reason for this may be the attractiveness of obtaining fees with less risk from the partnerships rather than directly engaging in card issuance.

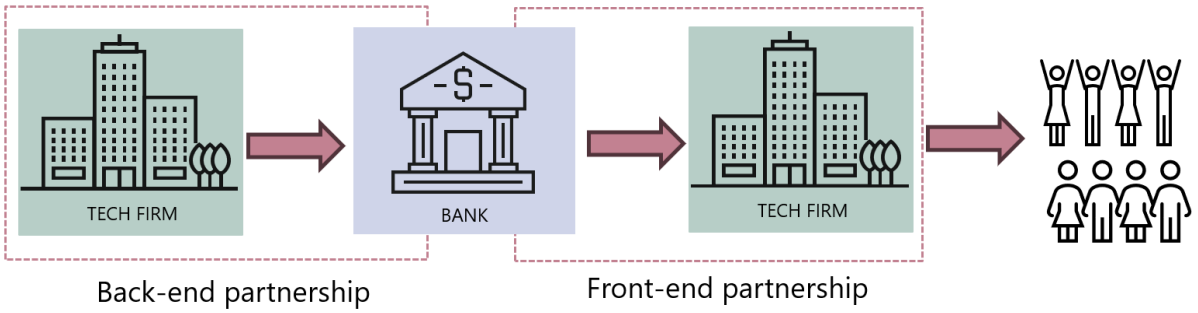
Section 3 – Partnership arrangements

31. **This section explores bank-tech partnerships in more detail.** The nature of partnerships between banks and tech firms is increasingly complex and opaque due to evolving arrangements and information challenges. This section therefore delves deeper into the different types of observed partnerships and the roles that banks and tech firms play and discusses associated benefits and risks.

Types of partnerships

32. **A bank partnering with a third-party, such as a tech firm, is nothing new.** Traditionally, partnerships between banks and tech firms focused on tech firms providing technology solutions for the bank's back and middle office functions, referred to as back-end partnerships. However, over time, various types of front-end partnerships have emerged and continued to evolve. In these partnerships, non-banks deliver banking products and services directly to customers (Figure 2).[48]

Types of partnership — Figure 2



Source: Adapted from BCBS (2024a).

33. **In back-end partnerships, a non-bank provides technology services to a bank.** This could include services such as software development, data storage, cloud computing, cyber security or artificial intelligence (AI) solutions. Essentially, in this model the bank remains the customer-facing entity and the tech firm, often referred to as the (technology) service provider, provides back-end technology services to

46 See European Commission (2021).

47 In August 2024, Amazon and Santander announced a partnership to launch the new Amazon Visa credit card in Germany. See Santander (2024).

48 The authors acknowledge there are other types of partnerships that may fall in between back-end and front-end partnerships, such as payment processors; however, these types of partnerships are not within the scope of this paper. In addition, a tech firm may be both a customer and partner of a bank, which may not always be clear-cut.

the bank.[49] Examples of this model include banks that have partnered with big techs, such as Amazon through Amazon Web Services and Google through Google Cloud, for cloud computing and data analytics services.[50]

34. **In front-end partnerships, a non-bank partners with a bank to deliver banking products or services to customers.** In this partnership arrangement, the non-bank partner engages directly with the customer, while the bank provides its infrastructure to operationalise the non-bank's offering of financial services.[51] This model can take many different forms, including what is often referred to as banking as a service (BaaS).[52]

- In a BaaS partnership arrangement, banking services are provided by a bank through a non-bank firm that markets, delivers or otherwise provides customers access to banking products and services.[53] This type of arrangement can be enabled directly through an application programming interface (API)[54] or secure file transfer protocol (SFTP).[55] It can also be enabled through another entity such as a BaaS platform provider or intermediary platform provider.[56] In this arrangement, the tech firm utilises the regulated bank's infrastructure, which includes the ability to accept deposits, extend credit, access payment networks and issue debit and credit cards, while the bank leverages the tech firm's technological capabilities and customer interface.[57]
- There are also other forms of front-end partnership arrangements in which the tech firm serves as an interface with customers. In these arrangements, the tech firm acts as an intermediary, facilitating direct interactions between the bank and its customers.[58] This includes credit referral partnerships or digital wallet services.

35. **Banks and tech firms have different motivations for entering into front-end partnership arrangements.** However, the common thread uniting them is their desire to remain competitive and relevant by meeting rapidly evolving customer demands for frictionless and seamless services, including banking services.[59]

- For tech firms, partnerships allow them to capitalise on the banks' franchise value,[60] infrastructure (such as the ability to accept deposits and access to the payment rails) and operational and

[49] Back-end partnerships have unique risk characteristics that are not a direct focus of this paper. These include banks' dependencies on big techs for cloud computing and data services resulting in concentration risks that could cause systemic effects in the case of a large-scale operational failure and a reduction of the ability of banks and regulatory authorities to assess whether services are being delivered in line with legal and regulatory obligations.

[50] See eg Deutsche Bank (2020) and BBVA (2023).

[51] FSB (2019c).

[52] Other terms frequently used in this context are "white labelling" and "embedded finance", though each carries a slightly different connotation.

[53] See BCBS (2024) and FBA (2024b).

[54] An API acts as a bridge, allowing non-bank firms to connect their platforms to a bank's systems. This connection enables non-banks to deliver and embed banking products within their digital platforms and under their own branding.

[55] SFTP is a network protocol for securely accessing, transferring and managing large files and sensitive data. See Gillis (2022).

[56] A BaaS platform or intermediary platform provider provides the technological infrastructure and platform needed to connect the bank with numerous other tech firms in order to deliver the banking product or service. This scenario is more common for smaller banks and tech firms. See BCBS (2024a).

[57] See US Department of the Treasury (2022) and Board of Governors of the Federal Reserve System (2023).

[58] FSB (2019).

[59] See also EBA (2018).

[60] By partnering with a bank, tech firms can leverage its franchise value, associating with an established banking brand and benefiting from the bank's reputation and customer trust. In some countries, however, customers might not be fully aware of a bank's role in the product offering.

financial expertise in managing financial operations, risk management and compliance. Apart from these benefits, tech firms' inclination to partner with banks may also be influenced by the existing regulatory framework and their desire not to be drawn too deeply into the regulatory perimeter.[61]

- For banks, tech partnerships provide them with access to innovative technology and related applications (eg user-friendly interfaces), which can aid their digital transformation efforts. Additionally, partnerships can enable banks to more quickly and cost-effectively launch products or services into the market, access new or expanded markets, generate new revenue sources and attract new customers.[62]

36. **A bank's size may also influence its motivation to enter into a front-end partnership with a tech firm.** For smaller, regional banks, partnering with a tech firm may be an appealing alternative to building technological capabilities in-house, especially when they lack the necessary resources. It allows them to reach new customer segments through the tech firm's digital platform. Larger banks, on the other hand, may be more restrained in entering certain front-end partnerships as they may have the capacity to develop their own technology or even acquire it from fintechs.[63]

37. **Back-end and front-end partnerships can potentially influence each other.** Where a big tech and a bank are in both types of partnerships, there may be implications for bargaining power dynamics and incentives. For example, the higher a bank's dependency on a big tech's back-end technological services, the more bargaining power the latter may have. Conversely, the higher the big tech's interest in not disturbing the relationship it has with its customers for back-end services such as cloud or AI solutions, the less willing it may be to enter into direct competition with them through front-end partnerships.

38. **The remainder of this section focuses on front-end partnerships.** Although back-end partnership arrangements play a crucial role within the banking value chain, they are not customer-oriented and have different characteristics. Also, their risk implications have been explored in more detail in other studies.[64] Therefore, in the rest of this section we outline the features of various front-end partnership arrangements and provide examples for deposit-taking, lending and payment partnerships. However, in practice these arrangements can involve more than one type of service offered to customers. Annex 1 provides further examples.

Front-end partnerships

Deposit-taking partnerships

39. **In deposit-taking partnership arrangements, tech firms establish a partnership with a bank that allows them to deliver depository products directly to their customers.** The customer typically completes the account opening application through the tech firm's digital platform and uses that same

[61] The regulatory regime may be stricter and more developed in some countries, and therefore may disincentivise big techs from obtaining their own licences. Respondents to a call for input issued by the FCA in November 2023 argued that big techs prefer to operate outside, or at the boundary of, the financial services perimeter as it minimises the amount of regulatory oversight placed on them (see FCA (2023a)).

[62] See FBA (2024b).

[63] An exception may be seen in the case of digital wallets operated by big tech firms. Large banks interviewed expressed a sense of inevitability in offering these to their customers, prompting questions about the true nature of such a "partnership".

[64] Risks include banks' reliance on big techs for cloud computing and data services, which may result in concentration risks that could trigger systemic effects in the event of a large-scale operational failure. It could also lead to a decrease in the capacity of banks and regulatory authorities to verify if services are being provided in compliance with legal and regulatory obligations. See eg Crisanto et al (2018, 2022) and Koh and Prenio (2023).

platform to access the deposit account. Thus, the customer may not engage directly with the bank itself and might only manage their account via the tech firm's digital platform.

40. **The tech firm often plays a pivotal role in maintaining the transactional system of record, while the actual deposits are held on the bank's balance sheet.**[65] There are a variety of ways in which deposits collected through a tech firm's platform can be held on a bank's balance sheet, including pooled custodial accounts and segregated accounts. The account setup determines, among other factors, whether and to what limit deposited funds are covered by deposit insurance guarantees. In the US, for example, the Federal Deposit Insurance Corporation (FDIC) allows for pass-through deposit insurance coverage if certain requirements, such as those related to bank account records, are satisfied.[66]

41. **Big techs' offering of deposit products through bank partnerships has so far been relatively limited.** In 2020, Google revealed plans to offer bank deposit accounts – Google Plexx – via their Google Pay app, in collaboration with several banks. However, these plans did not come to fruition, with Google subsequently stating it would concentrate on digital enablement for banks instead of providing financial services itself.[67] In 2023, Apple and Goldman Sachs Bank introduced a high-yield savings account product in the US. Within four months of its launch, Apple reported over $10 billion in deposits, demonstrating the rapid scalability potential of banking products delivered through a big tech platform.[68]

42. **Deposit-taking partnerships between fintechs and banks are more frequent.** For example, fintechs such as Chime in the US and Freo in India are delivering deposit services, such as checking accounts or business accounts, through their digital platform in partnership with banks. Some fintechs reportedly have millions of customers utilising these services. See Appendix 1 for additional details and examples.

Lending partnerships

43. **Tech firms and banks have entered into varying types of lending partnerships, typically for specific products.** The structure of these partnerships can vary. Some offer credit directly through the tech firm's digital platform, while others operate through referrals to a partnering bank. Credit products typically target retail and SME borrowers, focusing on specific market segments such as unsecured, short-term, or small-amount credit.[69]

44. **In a direct lending partnership, borrowers can access credit via a tech firm's digital platform.** Typically, in these arrangements a bank agrees to facilitate and fund loans, while the tech firm markets the lending product to customers and collects application data. The tech firm is able to capitalise on its digital platform and customer reach. The loan may be retained on the bank's balance sheet or sold back to the tech firm in whole or part, potentially with indemnification for the bank.[70]

45. **In the credit origination process, banks and tech firms play a range of roles.** The tech firm not only provides the front-end interface for borrowers to apply for a loan but also supports the lending

65 FBA (2024b).

66 FDIC (2024a,c).

67 Elias and Son (2021).

68 See Apple Newsroom (2023). However, there have been indications that this partnership may soon be dissolved, but details regarding the reason for the exit or how the partnership will be dissolved remain undisclosed. The reason for the potential termination of the partnership have not been announced, but public reports indicate the partnership will be dissolved in 12–15 months (see Staples (2024)).

69 Given the commonality of credit card partnerships, such as co-branded credit cards, amongst numerous entity types (eg airline companies, hotels and department stores), these partnerships were not included within the scope of this paper.

70 The tech firm might securitise any loans it acquires. However, through different contractual mechanisms, the bank may still maintain a financial stake in the loan performance. Typically, under these arrangements, the firm or a separate fourth party handles loan servicing and collection. See FBA (2024b).

bank by supplying information. The tech firm may generate this information by using alternative data and advanced credit risk models, including AI / machine learning (ML) models, to determine the credit worthiness of a borrower. Big techs may also use data from borrowers' non-financial interactions on the tech firm's digital platform, such as consumption levels. While these data are typically not shared with the bank, a credit assessment or score derived from them may be provided to assist the bank in its credit decision-making process.[71] However, despite having rich and diverse customer information, tech firms still lack the through-the-cycle credit experience and related data that are available to established banks.

46. **There are various examples for lending partnerships between banks and tech firms.** One is the lending partnerships between Ant Group and approximately 100 banks to provide them with credit assessment parameters (eg credit ratings) based on various data Ant Group has collected, to be utilised by the banks in their credit decision.[72] Google has also partnered with numerous banks in India to offer loans to individuals and merchants through their Google Pay app. Smaller fintechs are also partnering with banks to offer lending services, such as Atome in Singapore and Indifi in India.

47. **Another form of a lending partnership is a credit referral arrangement.** In this setup, both the tech firm and the bank interact with the customer. The tech firm, leveraging its access to customer data (eg merchant data) via its digital platform, acts as a broker to a bank, introducing eligible customers to specific lending products after conducting a pre-screening analysis.[73] Once eligibility is determined, the customer can opt to be redirected to the bank's website to complete the lending application. The bank is then responsible for the credit underwriting. An example of this credit referral model is the partnership between Amazon and ING in Germany. Amazon presents loan proposals on its lending page for eligible businesses that use its platform. Interested businesses are then directed to ING's website to submit a credit application, with ING deciding whether or not to extend credit.[74]

Payment partnerships

48. **Tech firms often rely on existing payment rails that can be accessed only by banks to deliver payment-related services.** In many countries, payment systems such as real-time gross settlement (RTGS) systems can be accessed only by domestic banks, thus requiring a relationship with a bank.[75] Alternatively, tech firms often provide payment services based on overlay systems which link a front-end application to a bank through the users' credit card or bank account.[76]

49. **In some countries, non-banks, including tech firms, can directly access payment systems or operate their own systems.** To access payment systems, tech firms typically need to be licensed and meet additional requirements.[77] For example, in India tech firms have access to the Unified Payments Interface (UPI), a mobile-based real-time payment system facilitating instant personal and merchant transactions.[78] However, to provide payment services, they may need to hold a licence (eg prepaid payment instruments (PPI) licence). One of the most popular UPI services is provided by Google Pay, which

[71] Ant Group Co., LTD, H Share IPO, 27 October 2020.

[72] Ant Group Co., LTD, H Share IPO, 27 October 2020.

[73] FCA (2022b).

[74] ING Newsroom (2020).

[75] A global survey of 82 central banks in the first quarter of 2021 found that only a minority of payment systems currently provide direct access to entities other than domestic banks (see CPMI (2022)).

[76] For a brief explanation of the arrangements for big tech payment services in Europe, see text box 1 in EBA (2021).

[77] These additional requirements are varied and include additional liquidity and solvency requirements, specific registration or licensing requirements, obtaining a foreign legal opinion, or fulfilling supplementary conditions as deemed necessary by the central bank if participation is seen to pose a high risk (usually connected to conflicting laws) (see CPMI (2022)).

[78] UPI processes over 75% of the country's retail digital payments. The UPI ecosystem currently features over 77 mobile applications including Google Pay, WhatsApp, Amazon Pay and more than 550 banks (see EPC (2024)).

allows users to conduct transactions, check their account balance and get insights about their spending habits.[79] Nevertheless, some tech firms operate "closed-loop" payment systems that do not interact with or depend much on existing payment infrastructure (eg AliPay, WeChat Pay, Vodafone M-Pesa and Mercado Pago).[80] In both of these cases, there is less need for bank partners.

50. **Against this backdrop, the nature of payment partnerships is highly diverse.** These partnerships may encompass various payment services across different parts in the value chain and may include the processing, clearing and settlement of transactions, as well as the acceptance, management and transfer of value. Common payment products include real-time payment solutions, co-branded debit/credit cards, e-money accounts/pre-paid cards, digital wallets and mobile payments, which can be made to a business or person.[81]

51. **Digital wallets are a prominent type of payment partnership.** The past decade saw strong growth in the worldwide usage of digital wallets such as PayPal, Apple Pay, Google Pay, Samsung Pay, WeChat Pay and Alipay.[82] Digital wallets allow customers to store their credit and/or debit cards within their personal devices to make payments both online and at the point of sale. In addition to these external options where e-wallets function as a conduit to banks, e-wallets may also offer "internal" payment options that may not necessarily involve a bank partner. These include: (i) buy-now-pay-later credit, (ii) e-wallet balances (ie e-money), and (iii) wealth-management products provided by e-wallet providers that function as interest-bearing demand deposits.[83]

Opportunities and risks

52. **Collaboration between banks and tech firms fosters innovation by capitalising on their relative advantages.** Tech firms' technological expertise may enhance the digital capabilities of banks striving to keep up with more convenient and user-friendly services to meet customer demands. Additionally, the services provided through these partnerships could potentially reduce costs and broaden the reach of financial services, even in geographic areas that were previously underserved or entirely without such services.[84] Overall, bank-tech partnerships may accelerate the digital transformation of the banking sector.

53. **While front-end partnership arrangements present opportunities, they also come with several risk considerations for banks and their supervisors.**[85] These arrangements may heighten risks across the bank, including financial, strategic, compliance, operational and reputational risks. The more services a bank provides in collaboration with others, the greater the need for truly effective third-party risk management processes to protect the bank's balance sheet and ensure activities are conducted safely and soundly, even in scenarios where the third party may fail to deliver its services.

[79] In India, the Google Wallet cannot store bank cards or be used to make digital payments, unlike in other countries (see Hindu Bureau (2024)).

[80] BIS (2020).

[81] That is, person-to-business (P2B), business-to-business (B2B), person-to-person (P2P) and business-to-person (B2P).

[82] E-wallets come in three types: closed e-wallets issued by a specific merchant or service provider (eg Amazon Pay), semi-closed e-wallets that allow users to make purchases at multiple merchants but lack widespread applicability (eg Alipay and Paytm), and open e-wallets that are issued by tech firms partnered with banks and allow users to make purchases at any merchant that accepts electronic payments (eg PayPal, Apple Pay and Google Pay) (see Bian et al (2023)).

[83] Bian et al (2023).

[84] For instance, evidence suggests that big tech lending has broadened access for small businesses. The use of machine learning and alternative data in credit assessments has also been linked to lower default rates, outperforming traditional models (see Cornelli et al (2023)).

[85] The discussion of risks in this section draws on BCBS (2024a).

54. **When multiple entities are involved in the offering of banking products and services, it can lead to a fragmented operational structure that increases operational risks.** In a partnership setting, a bank may not have full direct control over the services it provides, especially in situations where it faces challenges to effectively oversee and monitor its partner, eg due to a lack of transparency of their partner's proprietary technology. Moreover, a more fragmented operational structure places higher demands on a bank's resilience to cyber threats due to potentially greater susceptibility for cyber attacks or difficulties integrating new technologies into legacy IT systems.[86] Furthermore, like banks, tech firms often engage other entities, such as subcontractors, to provide services, adding another layer of oversight challenges, or "nth-party risk" for banks in monitoring the functions performed by these additional parties.[87]

55. **Operational complexity is further heighted when banks and tech firms rely on intermediary platform providers to connect them.** In such a scenario, the intermediary platform provider facilitates the connection between a bank and one or more tech firms to deliver banking products and services to customers. This arrangement further increases operational risks and complexity because it adds an additional layer between the bank and the customer. Additionally, the intermediate platform provider may be responsible for maintaining the transactional system of records, which could limit the bank's access to these records, potentially hindering its ability to assess its obligations or even causing delays in its customers' access.[88]

56. **Front-end partnerships may result in narrow banking models, raising questions about business model sustainability.** In cases where banks provide only a limited set of services to their tech partners, their business model may become less diversified, and they may develop significant asset and/or liability concentrations and come to rely on fee income that is generated by only a few sources. Rapid growth may also cause stress to capital ratios. Strategic risks may also arise where banks become overly dependent on tech firms for business origination, potentially losing control over volumes, product design and origination processes, while still being held accountable for risks.[89]

57. **Front-end partnerships can also introduce various compliance risks.** These include challenges in overseeing consumer protection obligations such as issues with timely dispute and error resolution, inaccurate representations of deposit insurance and other unfair, deceptive practices, or abusive acts or practices. Additionally, reliance on a third party to perform AML/CFT compliance functions such as "know your customer" (KYC) checks may increase the risk of the bank not meeting its AML/CFT regulatory requirements. While certain functions may be shared between a bank and a tech firm, the bank remains fully responsible for complying with applicable laws and regulations. This can be particularly challenging when the tech firm, acting as a distributor, has the incentive to support the activities on its platform regardless of whether regulatory requirements are met.

58. **Partnerships can introduce or accentuate a variety of other risks.** These include reputation risk, where the bank's image could be tarnished due to the actions of the partner tech firm.[90] Relatedly, banks may also have incentives beyond contractual obligation or equity ties to "step in" to support tech firms to which they are connected.[91] Moreover, banks could lose direct access to information by moving

[86] BCBS (2024a).

[87] BCBS (2024c).

[88] Board of Governors of the Federal Reserve System et al (2024).

[89] In front-end partnerships where banks do not have control over their customer relationships, they are exposed to the risk that the tech partners redirect their customer base elsewhere. This could lead to a sudden business loss for the bank, potentially having significant implications for the bank's liquidity and financial performance. See BCBS (2024a).

[90] BCBS (2024a).

[91] Step-in risk arises when a bank considers that it is likely to suffer a negative impact from the weakness or failure of an unconsolidated entity and concludes that this impact is best mitigated by stepping in to provide financial support (eg to avoid the reputational risk the bank would suffer otherwise) (see BCBS (2017)).

further away from their customers, which may pose challenges in effective decision-making and risk management.

59. **Front-end partnerships between banks and tech firms can pose risks for consumers.** Ineffective disclosures can lead to confusion about which entity – the bank or the tech firm – the consumer is actually contracting with. This confusion can extend to situations where consumers might be unsure about whom to contact if issues arise with a banking product or service. Additionally, in the event of a dispute, it may not be clear which entity's resolution process should be followed. This ambiguity can erode the consumer's trust in both the bank and the tech firm.

60. **Cultural differences between a tech firm and a bank can lead to divergent approaches in risk management.** Banks are mandated to adhere to robust risk management frameworks to deliver banking products and services in compliance with regulatory requirements. However, tech firms, often concentrated on growth and technological advancements, may not always prioritise risk and compliance culture or be familiar with the banking regulatory environment. This discrepancy can affect the bank and, in some cases, limit its ability to ensure compliance with its regulatory responsibilities.

61. **Tech firms, particularly big techs, wield significant negotiation power, which may result in terms that complicate banks' efforts to ensure banks are conducting activities in a safe and sound manner.** Tech firms may provide a bank with a spectrum of services, from back-end functions like cloud computing to front-end services related to deposit-taking, payment and lending. Consequently, the bank might become heavily reliant on the tech firm and may be inclined to accept overly restrictive terms. These terms could hinder the bank's ability to implement necessary measures to ensure robust compliance with regulatory obligations. For example, big techs might resist accepting certain provisions within contractual agreements with banks, such as audit clauses or third-party oversight requirements.

62. **Finally, partnerships can create other risks depending on the banking service provided.** These include:

- **Deposit-taking partnerships.** Deposits collected through third-party platforms may be less stable than core retail deposits, increasing their susceptibility to run risks. There may also be a concentration risk for the bank if these deposits are withdrawn simultaneously. This could occur if the tech firm transfers deposits to another bank or if negative news about the tech firm behind the platform circulates publicly. Furthermore, there may be customer confusion regarding deposit insurance. Customers may not be aware that their deposits might not be protected by a depository guarantee scheme in the event of a tech firm's failure when they are delivered through a tech firm.[92]
- **Lending partnerships.** In such partnerships, banks often utilise the tech firm's technological capabilities and data to assist in the credit decision-making process. Tech firms may employ complex and proprietary credit risk models that may be opaque to the banks and therefore a source of model risk, which has credit risk and compliance implications. Tech firms may also be hesitant to provide bank personnel with access to their proprietary models for testing and validation. This, coupled with potential resource limitations on the bank's side, could present challenges for banks in understanding such models and complying with their own model risk management processes. Misaligned incentives, where the bank may bear more of the credit risk while the tech firm earns referral fees for every new borrower, can also present challenges. Furthermore, lending through partnerships may arguably fall under the category of transactional banking, which tends to be more procyclical than relationship banking due to the absence of long-term client relationships.

[92] For example, in the US deposit insurance misrepresentations may occur when non-bank third parties communicate to end users that their funds are FDIC-insured, without disclosing that FDIC insurance protects only against the failure of an insured depository institution, and not against the failure of the non-bank entity.

- **Payment partnerships.** Providing payment services through partnerships can expose banks to risks that they would not face if they were operating independently. Operational losses can occur from unauthorised payment activity through the tech firm's interface, leading to charges that the bank may have to absorb. In some cases, banks may be required to refund payments and related fees to customers, and these amounts may not be recoverable. Furthermore, system disruptions or failures at the tech firm can delay processing, introduce errors and present other risks such as liquidity or credit risk to the bank.[93] Additionally, the responsibility of resolving disputes and errors may not always be clear among all parties, leading to delays and losses and potential customer confusion.

Section 4 – Implications for the value chain

63. **The entry of tech firms into banking services, whether through partnerships with banks or monoline licences, has resulted in the emergence of a new banking value chain.** Today's consumers seek financial services that are customer-centric, user-friendly, frictionless, paperless, cost-effective and readily available. As a result, there is a growing preference, especially among younger and underbanked demographics, for banking services accessible via tech firms.[94] As discussed in previous sections, tech firms often provide these services through front-end partnerships and monoline licences. However, this modus operandi contrasts with the traditional role of tech firms as third-party providers supporting banks' back office functions.[95] It also contrasts with the linear and vertically integrated business model that banks have traditionally followed.

64. **The conventional banking business model operates on an integrated, vertical value chain.** This model, depicted in Figure 3, begins with the bank's balance sheet and the permission by regulatory authorities to provide banking services. This is followed by the infrastructure for providing banking services, such as accessing payment and settlement systems, and performing other functions. The middle and back office function – which includes accounting, recordkeeping, technology services, credit decisioning and regulatory compliance – then processes these services. The value chain concludes with the customer interface and delivery, which encompasses customer engagement and the provision of core banking services.[96] In this model, the bank owns the value chain end to end and serves as a one-stop shop for banking services, and all parts of the value chain fall within the banking regulatory perimeter.[97, 98]

93 For a detailed discussion on risks associated with payment systems, see OCC (2021).

94 This is particularly evident in countries or areas where banks have limited reach.

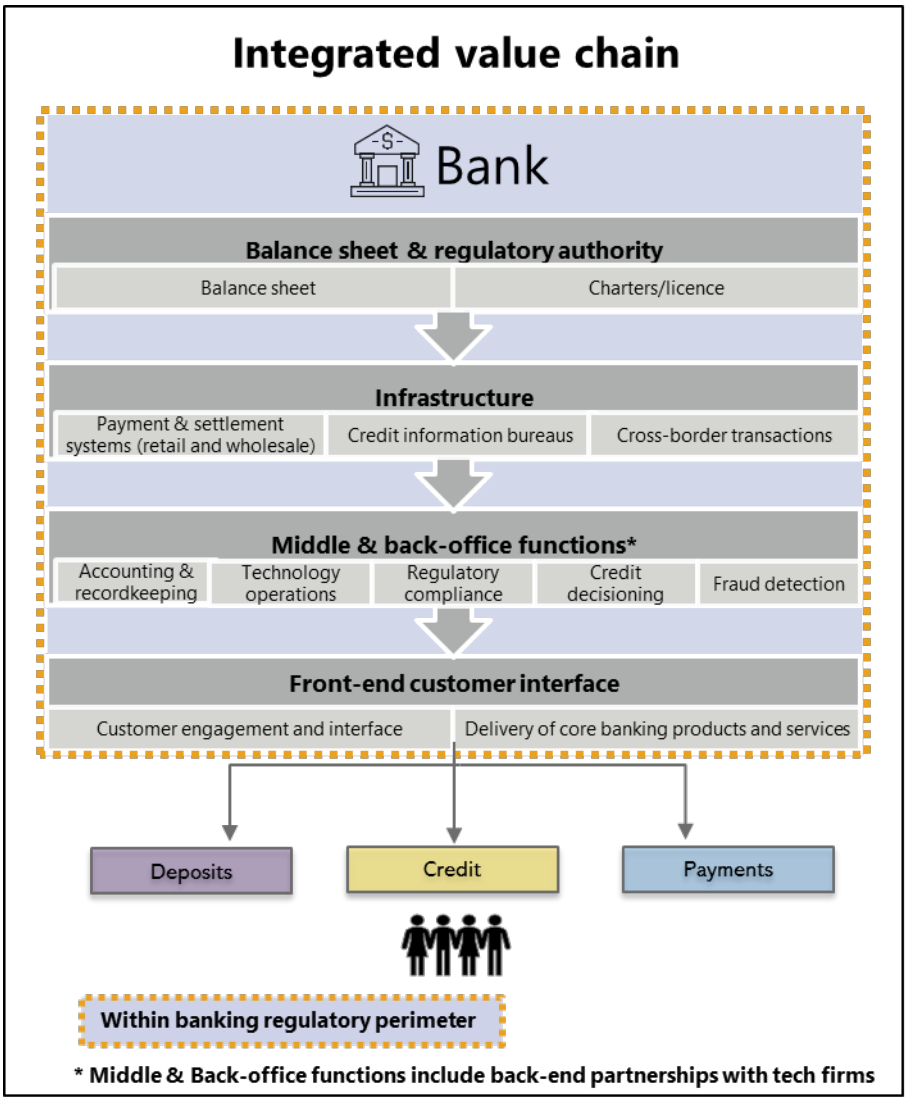
95 Tech firms may partner with multiple banks to provide specific banking services, thereby enhancing customer convenience and increasing the value of their platforms.

96 See Feyen et al (2021).

97 US Department of the Treasury (2022).

98 Tech firms with a digital banking licence do not disrupt this value chain, as all layers and services remain under the same entity's control and within the regulatory perimeter.

Integrated value chain Figure 3



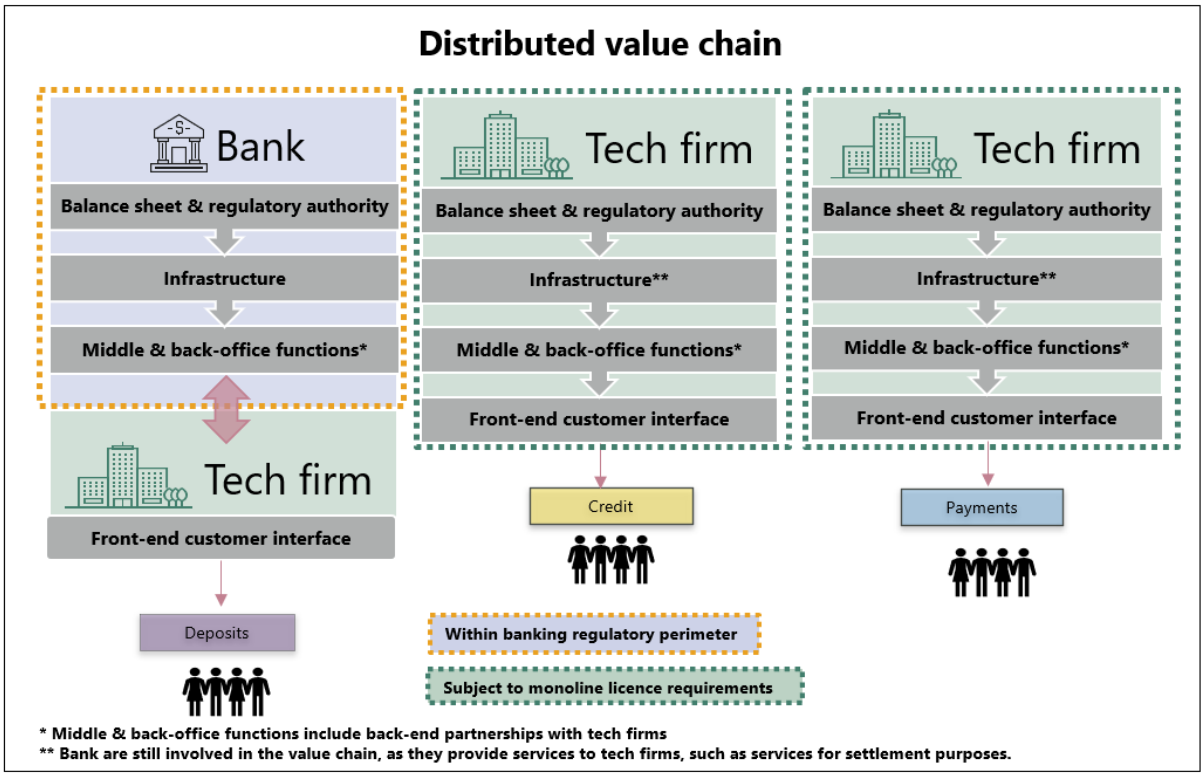
Source: Authors' conceptualisation based on US Department of Treasury (2022) and Feyen (2021).

65. **As tech firms offer banking services by forming partnerships with banks or securing monoline licences, they create a new value chain, one that is further extended and expanded.** In this new value chain, banking products are unbundled and produced and/or delivered by more than one entity (Figure 4). In partnerships (eg for deposit-taking), the front-end customer interface is no longer with the bank and the tech firm delivering these services is outside the banking regulatory perimeter. Also, if payment and/or lending services are offered via monoline licences, they may also be outside the banking regulatory perimeter.[99]

[99] Depending on the regulatory framework, this may not apply in jurisdictions where the banking regulatory framework extends to holders of monoline licences.

Distributed value chain

Figure 4



In this distributed value chain, there are numerous possible scenarios for tech firms to provide access to banking services. This may be done through partnerships with banks to deliver depository, lending or payment services or through monoline licences for payment and/or lending services. The depiction is a reflection of one potential example. In this example, a tech firm provides: (i) access to depository services through a bank partnership; (ii) payment-related services through a payment licence; and (iii) credit products through a non-bank lending licence.

Source: Authors' conceptualisation based on US Department of Treasury (2022) and Feyen (2021).

66. **While banks are pushed further away from the direct customer relationship in this new banking value chain, they continue to play an important role.** In partnerships, banks utilise their infrastructure to allow tech firms to give customers access to banking services. Furthermore, when tech firms directly provide banking services to customers through monoline licences, banks typically remain involved in at least one layer of the value chain.[100] For example, in payments many countries restrict access to payment systems, such as RTGS, to banks. This means tech firms require a bank account (eg merchant account) to facilitate payments.[101] Similarly, in credit a tech firm's lending activities may be funded by banks through credit or liquidity facilities.

67. **A more distributed value chain offers several potential benefits, such as fostering competition and efficiencies in the delivery of banking products and services; however, it also presents challenges.** When multiple entities are involved in the production and delivery of banking products, operational and compliance issues (including for consumer protection) become a significant concern. In a traditional vertically integrated bank, accountability is clear when issues arise. However, when the value chain is spread across multiple players – such as a bank and a tech firm involved in the customer relationship, another entity holding customer funds, a third providing data analytics and a fourth providing technology infrastructure – it can become difficult for the parties to determine accountability for any

[100] Brainard (2017).

[101] However, some countries are now exploring broadening access of non-bank payment service providers, including tech firms (see CPMI (2022)).

mishaps or misdeeds. Relatedly, customers may face confusion about which entity is offering a banking product and who to engage with regarding its management.

68. **The distributed value chain may also give rise to data privacy and security concerns.** The complexity of partnerships and interdependencies within a distributed value chain may increase banks' data governance risk. While strict requirements on data use apply in several jurisdictions, there could be potential challenges for privacy and consent, particularly when customer data are used in ways that customers do not fully understand or that were not initially intended. Challenges may also arise in relation to data security and protection as various parties access the banks' data. Finally, issues around data ownership and accessibility may inhibit the bank's ability to meet its regulatory requirements.[102]

69. **Against the backdrop of this distributed value chain, big techs have come to offer various banking services in one place.** Over time, they have expanded their financial service offerings on their digital platforms or super apps, giving the impression of a rebundling of banking services. However, despite being accessible in one place, these services are produced based on a distributed value chain and primarily focus on specific products that complement their overall business model, such as low-value, short-term credit products for e-commerce. This selective approach leaves a gap for traditional banks to fill, particularly in areas like long-term financing and relationship-focused services. Therefore, despite big techs' involvement in the banking value chain, many banking service needs are still predominantly met by incumbent banks.

70. **Going forward, the distributed value chain will play a role in the future of banking.** In 2018, the BCBS developed five forward-looking scenarios, based on: (i) which actor manages the customer relationship or interface; and (ii) which actor ultimately provides core banking services, and manages the risk.[103]

71. **The aforementioned developments can be seen as a combination of the scenarios developed by the BCBS.** The use of monoline licences and partnerships, especially for services that require a banking licence, has led to a more modular approach to delivering financial services. This delivery is often distributed across multiple entities, with banks usually remaining engaged in at least one layer of the value chain. Tech firms, on the other hand, often maintain the direct customer relationship, leveraging customer-facing digital platforms to distribute banking services. When viewed collectively, these developments arguably reflect elements of the "distributed bank"[104] and "relegated bank"[105] scenarios.

72. **Taken together, these developments are prompting questions about how best to respond.** The existing regulatory framework may not fully account for the additional risks brought about by a more distributed value chain. For those risks not yet fully addressed, the overarching question for authorities is

[102] See BCBS (2024a).

[103] The five scenarios are: the better bank (modernisation and digitisation of incumbent players), the new bank (replacement of incumbents by challenger banks), the distributed bank (fragmentation of financial services among specialised fintech firms and incumbent banks), the relegated bank (bank's relegation to providing only specific services without owning the customer relationship) and the disintermediated bank (direct interaction of customers with individual financial service providers). The BCBS noted that future evolution is likely to be a combination of these scenarios, which seems to be supported by the impact of tech firms' activities in banking on the value chain (BCBS (2018)).

[104] In this scenario, financial services are provided by both incumbent banks and tech firms. They have the ability to seamlessly integrate their services through digital customer interfaces and collaborate through various structures, such as partnerships. The ownership of the customer interface itself can be attributed to any of the players in the market. It is facilitated by open APIs and customers may use multiple financial service providers.

[105] Under this scenario, incumbent banks become commoditised service providers and relinquish direct customer relationships to tech firms which utilise customer-facing digital platforms to offer a wide range of financial services from multiple providers. Tech firms rely on incumbent banks for their banking licences to provide essential banking services.

what policy response to pursue and where to direct attention.[106] The following section discusses examples of policy responses across jurisdictions and areas that require further consideration.

Section 5 – Policy responses and further considerations

Evolution of policy responses

73. **Authorities have implemented various policy responses to address the impact of tech firms' activities in banking and a more distributed value chain.** These policy responses include initiatives to: (i) gather more information; (ii) adjust prudential/conduct requirements or clarify supervisory expectations in different policy areas (ie operational resilience, financial soundness, consumer protection, AML/CFT and competition); and (iii) review the regulatory perimeter and supervisory approach. The following section highlights examples of policy responses in each of these domains.

Information-gathering

74. **Several authorities have recently embarked on initiatives aimed at gaining a deeper understanding of the implications of tech firms' involvement in financial services, including those stemming from front-end partnerships.** While some of these initiatives are broad in their scope, others are more focused, targeting specific topics. For instance:

- In February 2024, the European Supervisory Authorities (ESAs) released a review of big techs' direct financial services provision in the EU.[107] The report underscores several regulatory and supervisory challenges, such as difficulties in identifying front-end partnerships and understanding their associated opportunities and risks. Moving forward, the ESAs plan to enhance the monitoring of big tech activities by creating a data mapping tool within the European Forum for Innovation Facilitators (EFIF).[108] This tool is intended to provide a framework for ongoing monitoring of big techs' direct and indirect relevance to the EU financial sector.[109] Additionally, the ESAs plan to continue interdisciplinary exchanges within the EFIF setting to promote information-sharing between EFIF members and other relevant financial and non-financial authorities, such as data protection and consumer protection authorities.
- In July 2024, the US Federal Banking Agencies issued a request for information (RFI) on arrangements where financial technology companies collaborate with banks to offer banking products and services to consumers and businesses. The RFI notes that supervisory experience has revealed a variety of potential risks with these arrangements and seeks input on the nature of bank-fintech arrangements, effective risk management practices and implications of such

[106] Arguably, neither a tech firm's entry in banking nor the policy response is exogeneous.

[107] Among other things, the report suggests that the growth of partnerships between big tech companies and financial institutions could pose certain risks. See ESA (2024).

[108] The EFIF was established following the 2019 Joint ESA report on regulatory sandboxes and innovation hubs, which identified the need for greater coordination and cooperation between innovation facilitators to support the scaling-up of fintech across the EU single market (see ESMA (2024)).

[109] This monitoring matrix aims to provide a dynamic, detailed framework for monitoring the type and scale of direct financial service activities provided by big techs in the EU. This includes aspects such as cross-border activity, the number of subsidiaries engaged in providing relevant financial services and other roles in the financial sector. Additionally, it considers their role as key technology providers, including being designated as "critical third-party providers" under the Digital Operational Resilience Act (DORA), as well as the provision of gatekeeper platform services under the Digital Markets Act.

arrangements. It also invites suggestions on whether enhancements to existing supervisory guidance could be beneficial in managing risks associated with these collaborations.[110]

- In July 2024, the UK Financial Conduct Authority (FCA) and Payment Systems Regulator (PSR) issued a *Call for Information* to better understand the opportunities and risks that digital wallets create. Specifically, the authorities are requesting information on: (i) the range of benefits that digital wallets bring for service users; (ii) whether there are any features that mean payments are not working as well as they could for consumers and/or businesses; (iii) their role in unlocking the potential of account-to-account payments and how they could affect competition between payment systems; and (iv) whether digital wallets could raise any significant competition, consumer protection or market integrity issues, either now or in the future.[111]

Prudential and conduct requirements

75. **Several policy initiatives have been introduced to modify aspects of prudential and conduct regulatory frameworks.** In general, there are two regulatory strategies. One is to incorporate the banking activities of tech firms within existing rules, and the other is to create new targeted requirements. Some of these requirements impose restrictions on how an activity can be performed, irrespective of the type of entity performing the activity ("activity-based measures"). Others aim to acknowledge the aggregate risk of an entity across all its activities by constraining a combination of activities at the entity level ("entity-based measures").[112] The initiatives that follow incorporate both approaches.

Operational resilience

76. **Policy initiatives targeting operational resilience have mostly focused on the back end of the value chain.** At the international level, standard-setting bodies have taken steps to address the growing dependence of banks on third-party service providers. The BCBS, for example, has recently issued for consultation principles for the sound management of third-party risk. At the national level, several measures are being implemented to enhance operational resilience. These efforts include the full adoption of the principles for operational resilience (POR) and revised principles for sound management of operational risk (PSMOR) and, in some jurisdictions, the introduction of a new regulatory regime for critical service providers. These policy initiatives are primarily focused on the risks banks face from outsourcing and third-party services and, as such, mainly address operational risks at the back-end of the value chain (Box 2).

77. **Initiatives specifically aimed at addressing operational risks from front-end partnerships are relatively scarce.** In the US, the federal banking agencies recently issued a joint statement flagging potential risks in certain front-end partnerships used to deliver bank deposits products and services, which also highlights examples of effective risk management practices that banks may consider when managing operational implications of these arrangements.[113] In China, requirements for managing operational risks are included in its regulatory framework for FHCs, which applies to firms, including tech firms, that have

[110] In this context, the RFI underscores the agencies' support for responsible innovation and third-party banking arrangements, provided they are managed in accordance with safe and sound practices and comply with applicable laws and regulations.

[111] FCA (2024b).

[112] See Restoy (2021) and Borio et al (2022).

[113] These include: (i) developing and maintaining risk-based contingency plans that address potential operational disruptions or business failures at the third party, which may affect end users' access to funds; (ii) implementing internal controls to mitigate risks inherent in deposit functions, which may include dual control and separation of duties, payment data verification and clear error processing and problem resolution procedures; and (iii) maintaining a clear understanding of any management information system that supports the activity is crucial, especially when the deposit and transaction system is managed through a third party or subcontractor. See FBA (2024a).

two or more different types of financial services companies that exceed certain size thresholds.[114] In India, the RBI's Guidance Note on Operational Risk Management and Operational Resilience includes expectations with regard to front-end partnerships.[115]

Box 2

Policy initiatives to address banks' reliance on third-party service providers

At the international level, policymakers are acting to respond to the increasing reliance of banks on third-party service providers. In 2023, the FSB published a toolkit for financial authorities and financial institutions for enhancing their third-party risk management and oversight. Other standard-setting bodies, such as the International Organization of Securities Commissions and the International Association of Insurance Supervisors, have also developed international standards and guidance addressing third-party risk management in the financial sector.① For the banking sector, in 2021 the BCBS released revisions to the PSMOR and *Principles for operational resilience* (POR) to enhance banks' ability to withstand operational risk-related events that could cause significant operational failures or disrupt financial markets.②

The BCBS has recently taken additional action to address the growing dependence of banks on third-party service providers. In April 2024, the Committee published a revised version of its *Core principles for effective banking supervision* which includes the introduction of a new Principle 25 on operational risk and operational resilience.③ In July 2024, the BCBS issued for consultation principles for the sound management of third-party risk (proposed Principles) which seek to promote a principles-based approach to improving banks' operational risk management and operational resilience through effective third-party risk management.④

At the national level, significant efforts are being made to bolster operational resilience. Following the Covid-19 pandemic, the operational resilience of banks has become a key supervisory priority in many countries. For example, in 2023 the US Federal Banking Agencies issued unified guidance on managing risks associated with third-party relationships, which was further supplemented by a guide specifically for community banks released in 2024.⑤ In India, the RBI has implemented outsourcing guidelines that restrict banks' outsourcing of certain critical functions. These include core management functions such as internal audit, compliance and decision-making functions (eg determining compliance with KYC norms, approving loans and managing investment portfolios). Efforts at the national level also include the full adoption of the POR and revised PSMOR.⑥

In addition, some authorities are gaining powers to supervise critical service providers. In some jurisdictions, supervisory authorities have or are in the process of acquiring powers to supervise the provision of certain critical services by third-party service providers, such as those deemed to give rise to systemic third-party dependencies.⑦ This is the case in the EU, where tech firms are subject to direct oversight under the Digital Operational Resilience Act (DORA).⑧ In the UK, the Financial Services and Markets Act (FSMA) 2023 granted HM Treasury new powers to designate service providers as critical third-party providers if a failure in, or disruption to, the services they provide to financial services firms would pose a threat to financial stability or confidence in the UK financial system.⑨

While these policy initiatives have mostly focused on back-end partnerships, they are relevant for front-end partnerships too. The FSB Toolkit as well as the BCBS proposed Principles define third-party service relationships as arrangements for service provision to financial institutions. As such, they primarily address situations in which a bank is the recipient of third-party services, and not those in which the bank provides services to others. Similarly, operational risk requirements tend to focus on risks to banks from outsourcing and third-party service relationships at the back end, rather than on operational risks throughout the entire value chain. Despite these requirements addressing only a segment of the value chain, they lay crucial groundwork for banks to maintain operational soundness, which is vital for their role in front-end partnerships.⑩

① See Annex 1 in FSB (2023). ② While the PSMOR set forth principles for operational risk management, the POR aims to foster a principles-based approach to enhance operational resilience as an outcome of effectively managing operational risks that could emerge from

[114] For instance, an FHC is required to establish a robust group-level "risk isolation mechanism" that prevents and addresses risks from, inter alia, sharing IT and operating systems. See Article 34 in PBC (2020).

[115] RBI (2024).

disruptions. See BCBS (2023). ③ BCBS (2024). ④ The proposed Principles would replace the Joint Forum Paper Outsourcing in Financial Services published in 2005 and complement and expand upon the FSB's aforementioned toolkit. ⑤ The 2023 guidance offers the agencies' views on sound risk management principles for banking organisations when developing and implementing risk management practices for all stages in the life cycle of third-party relationships, including those with fintech companies (Federal Register (2023)). The guide for community banks is intended to assist community banks when developing and implementing their third-party risk-management practices (FBA (2024c)). ⑥ In November 2023, the BCBS found that the effectiveness and maturity of their adoption vary across banks and jurisdictions, and that the management of third parties and dependencies, as well as the alignment of third parties with resilience expectations, are considered to be among the most significant challenges for banks. See BCBS (2023). ⑦ See Annex 2 in FSB (2023). ⑧ In the US, the provision of certain services to a bank by a third-party service provider is also subject to limited direct oversight under the Bank Service Company Act. See also Box 1 in Annex 2 in FSB (2023). ⑨ FCA (2023d). ⑩ The BCBS consultation for the sound management of third-party risk notes that "[p]rinciples in this document could also provide value for other types of relationships that banks may have with third parties, including joint support for banking products".

Financial soundness

78. **Some authorities have implemented a blend of measures to address prudential concerns from partnerships.** China, which has been the most active in this field, has taken regulatory actions based on the principle that tech firms: (i) must obtain appropriate licences before they can legally engage in financial activities; and (ii) should be regulated according to the nature of their business and risk profiles, a concept referred to as "substance over form". Specific approaches include a set of measures aimed at ensuring that partnerships do not significantly increase the risk profile of the banks. Another set seeks to prevent banks from violating regulatory requirements through entering partnerships. A further measure mandates risk-sharing between digital lenders and partnered banks, and limits online loan amounts. Box 3 provides an overview of the measures taken in China.

79. **The US Federal Banking Agencies have underscored the implications of deposit-taking partnerships for managing a bank's growth, liquidity and capital.** In particular, they highlighted the need for banks to establish concentration limits, diversification strategies, liquidity risk management strategies and exit strategies, as well as maintain capital adequacy.[116] They also highlight the need for banks to analyse whether parties involved in the placement of deposits meet the definition of a deposit broker and report any such deposits as brokered deposits.[117] In addition, banks are expected to assess the third party's financial condition, including access to funds, earnings and expected growth.[118]

Box 3

China: regulatory response to tech firms' activities in the financial sector

China's regulatory framework has evolved over the years, beginning as an accommodative regulatory environment for tech firms in the 2000s to early 2020s. This resulted in numerous tech firms providing financial services that brought efficiencies, cost reduction and financial inclusion. However, it has also resulted in concerns around regulatory arbitrage, and some tech firms have obtained dominant market positions. In response, in the early 2020s China began developing a regulatory framework that focused on big techs' financial services, antitrust and data protection. In addition, Chinese regulators introduced a mix of measures for all three banking services.

Deposits. Over the last few years, Chinese authorities observed a trend of small local banks taking deposits nationwide through third-party online platforms and noted several concerns with this practice. First, the reliance on online deposits pushed up funding costs for banks, potentially tempting them to take on riskier investments. It also increased liquidity risks as online deposits were less sticky and small banks could struggle to manage the sudden influx of deposits. As such, online platforms operated by tech firms became a "risk amplifier". Second, in terms of

[116] This may include contingency funding plans that describe how the bank will respond to customers' unexpected deposit withdrawals and reasonable assumptions, such as non-maturity deposit customer behaviour.

[117] FBA (2024a).

[118] Federal Register (2023).

compliance, local banks are supposed to operate within their designated regions. By accepting nationwide deposits, they were acting like national banks without proper authorisation which may also be seen as a form of abuse of the deposit insurance scheme. In addition, tech platforms intermediating deposits online could be seen as offering brokerage services without proper authorisation.

In response, in January 2021 the former Chinese Banking and Insurance Regulatory Commission (CBIRC) and the People's Bank of China (PBC) stepped in and banned this practice.① Since then, banks and tech firms are no longer allowed to partner to collect online deposits, and outstanding amounts have to be wound down over time.

Payments. Since 2010, tech firms like Ant Group and Tencent have partnered with banks to offer fast payment services, with customers being able to link their payment accounts to their bank cards without needing to log in to their online banking every time.

In 2019, the PBC introduced two key regulations in response to the growing influence of non-bank payment service providers. These regulations target the management of clients' pending payments, which are funds: (i) received in advance by non-bank payment institutions for handling the payment entrusted by customers; and (ii) that are not the property of the payment institutions. The first regulation mandates that tech firms deposit 100% of customer balances held in commercial banks into reserve accounts with the PBC, curtailing tech firms' capacity to excessively profit from the interest rate spread on these funds. The second regulation stipulates that transactions are to be settled solely through PBC accounts, and cross-institutional transactions must go through clearing institutions.② This prevents tech firms from using these reserves for credit extension or investment activities, thereby ensuring these funds remain readily available for customer transactions.

Credit. Through their online platforms, tech firms help commercial banks to attract customers, sell products, analyse data and manage loans. Additionally, non-bank lenders affiliated with tech firms also cooperate with banks to issue loans. The increase in online loans originated by bank-tech partnerships prompted financial regulators to take a number of measures. In 2021, financial regulators banned local banks from conducting online lending business outside their designated regions. They also required commercial banks to have substantial risk-sharing with their tech partners: (i) tech firms must contribute at least 30% of the funding for any loan issued jointly with a commercial bank; (ii) online loans issued by a bank through any single platform cannot exceed 25% of the bank's Tier 1 capital; and (iii) the total balance of online loans issued jointly by a bank with all its tech partners cannot exceed 50% of total outstanding loans.

In addition, banks frequently partner with tech firms to issue credit cards, capitalising on their expertise in attracting and retaining customers. Recognising this trend, financial regulators closely monitor these collaborations, focusing on marketing activities, credit standards, risk management and the flow of funds related to such activities.

① CBIRC and PBC (2021). ② Global Times (2021a).

Consumer protection

80. **Consumer protection remains a critical regulatory consideration.** While banks are subject to consumer protection requirements regardless of their partnerships with tech firms, several authorities have undertaken a variety of measures to address issues they have identified. For example:

- **Warnings.** Some authorities have issued warnings about misleading adverts regarding products tech firms offer, or tech firms' practices. For example, in 2022 the FCA issued a warning to firms offering BNPL products, clarifying that while some BNPL agreements are unregulated, the financial promotions for all BNPL products must adhere to the financial promotion rules.[119] In the same year, the BNPL Code was launched by the Singapore FinTech Association and industry players, under the guidance of the MAS. The Code formalises a set of safeguards to mitigate the risk of consumer over-indebtedness arising from the use of BNPL services. Also in 2022, the US Consumer Financial Protection Bureau (CFPB) warned big techs that they must adhere to federal consumer financial protection laws when using sophisticated behavioural targeting techniques to market financial products.[120]

[119] FCA (2022a).

[120] CFPB (2022).

- **Misrepresentation of deposit insurance.** In deposit-taking partnerships, there is a heightened risk of "customer confusion" related to deposit insurance coverage, which may be exacerbated by marketing materials or other statements of a bank's partner. End users may not be aware that access to their funds may depend on the third party and that deposit insurance does not protect against losses resulting from the failure of the third party. In this context, in 2024 the FDIC amended its regulation governing the use of the official FDIC sign and insured depository institutions' advertising statements and clarified regulations regarding misrepresentation of deposit insurance.[121] Additionally, US federal banking regulators restated existing expectations towards banks. They expect them to: (i) establish policies and procedures and develop prudent risk management practices for certain deposit-related arrangements to avoid misrepresentation of deposit insurance; and (ii) ensure such policies and procedures include, as appropriate, provisions related to monitoring and evaluating activities of persons that facilitate access to the bank's deposit related services or products to other parties.[122]
- **New conduct requirements.** In India, the RBI introduced customer protection and conduct requirements for digital lending in 2022.[123] These require regulated entities (eg banks) and their lending service providers (eg tech firms) to appoint a nodal grievance redressal officer to handle complaints, including those against their respective digital lending apps.[124] In lending partnerships, all documentation must be on the bank's letterhead to ensure customers are aware of the bank they are dealing with. Additionally, banks are required to publish a list of tech companies with which they partner, along with the activities in which these companies are engaged, on their websites. The bank is solely responsible for credit sanctions and all loan disbursements, and repayments must be conducted solely between the bank accounts of the borrower and the regulated entity, without involving any pass-through or pool account of the lending service provider or any third party.[125] The guidelines also lay down several data privacy and protection measures to safeguard customer data.
- **Enforcement action.** In the US, the CFPB has used its authority to take direct action against fintechs that violate consumer financial laws. This includes ensuring consumers have timely access to their funds and prevents unfair, deceptive or abusive acts or practices. For instance, the CFPB has issued monetary fines against fintechs and required redress to affected customers as a result of a fintech violating consumer protections.[126]

[121] FDIC (2024b).

[122] FBA (2024b).

[123] These requirements, which are part of the RBI's guidelines for digital lending, were implemented following recommendations from a 2021 working group on digital lending including lending through online platforms and mobile apps (see RBI (2021)).

[124] Contact details prominently indicated on the website of the regulated entity, its lending service provider and on digital lending apps (see RBI (2022)).

[125] Also, any fees or charges payable to lending service providers in the credit intermediation process should be directly paid for by the regulated entity, not by the borrower.

[126] CFPB (2024).

AML/CFT

81. **Partnerships may give rise to several challenges in terms of AML/CFT compliance.** These challenges largely depend on the nature of the relationship between the bank and its technology partner, as well as the specific products, services and activities that are offered through the partnership. One challenge is that banks and tech firms may be subject to different AML/CFT requirements. For instance, in the US banks are required to comply with the Customer Identification Program and Customer Due Diligence rules. However, these rules do not necessarily apply to tech firms.[127] Another potential issue is risk oversight, especially if information is not freely exchanged between the bank and the tech company.

82. **With a few exceptions, regulators have generally not issued specific guidance regarding bank-tech partnerships.** However, the principle is that the bank is ultimately responsible for AML/CFT requirements. For instance, the EBA has issued specific guidance on third party reliance for AML/CFT purposes.[128] In the US, the Federal Banking Agencies have issued enforcement actions against banks with tech partnerships that are not complying with AML/CFT requirements, communicating the regulatory expectations for AML/CFT compliance.[129] These actions emphasise that banks will be held accountable for managing AML/CFT risks associated with their partnerships. They also outline controls and risk management principles to handle AML/CFT risks in partnerships, including: (i) conducting risk assessments before entering into a partnership and throughout its duration; (ii) conducting initial and ongoing due diligence of tech partners; (iii) establishing and maintaining clear policies and procedures for third-party risk management; and (iv) contractually managing and allocating risks.[130]

Competition

83. **Several jurisdictions are in the process of adopting ex ante competition requirements to ensure tech firms follow fair business practices.** These requirements, aimed at pre-emptively constraining the business practices of tech firms, include ensuring the interoperability of online platforms with third-party entities, prohibiting restrictions on business users interacting with their customers or offering products outside the platforms, and mandating equal treatment for all existing and potential business users on the platforms.[131] In the UK, these measures have been embodied in the Digital Markets, Competition and Consumers Bill, introduced in Parliament in April 2023. In the EU, the Digital Markets Act (DMA) was enacted in November 2022 to similar effect. Comparable regulatory regimes are also under development in other jurisdictions, including Australia, Japan, Korea and the US.[132]

84. **Against this backdrop, several authorities are taking steps to address competition issues.** These include assessing their regulatory frameworks or supervisory practices in relation to competition issues and establishing new organisational units to promote competition. For example:

- **Review of financial services legislation.** In a review of the EU's regulation of payment services, the European Commission found that the existing rules under PSD2 may allow big techs to hinder or distort competition. As a result, the review puts forth a series of recommendations, including the creation of a public, distributed register to document the outcomes of antitrust investigations; and regular meetings between the ECB, national central banks and antitrust

127 Stipano et al (2023).

128 EBA (2022b, 2023, 2024).

129 FDIC and Ohio Department of Commerce (2024) and OCC (2022).

130 Similarly, a joint statement issued by the US Federal Banking Agencies in July 2024 highlights that banks are expected to have adequate policies, procedures, oversight and controls to help ensure compliance with applicable AML/CFT requirements, such as monitoring for and reporting suspicious activity, customer identification programmes and customer due diligence (FBA (2024a)).

131 Crisanto, Ehrentraud, Lawson and Restoy (2021).

132 FCA (2023a).

authorities. Moreover, the European Parliament should be consistently updated on the outcomes of competition investigations into big techs conducted at the national level.[133] Furthermore, the European Commission proposed a new framework for Financial Data Access (FiDA) in 2023. This framework would enable firms to access a broad spectrum of personal financial information from both banks (which are already required to enable other companies access to basic client data) and NBFIs, including tech firms. Among other policy objectives, enabling broader access to customer data is expected to stimulate competition in the financial sector.[134]

- **Review of the role of data for competition.** In November 2023, the FCA published a call for input, asking for information on whether any data asymmetry between big techs and financial services firms could influence how competition evolves in financial services markets.[135] Although the call for input did not uncover any significant immediate effects of this data asymmetry, it emphasised three potential issues that could negatively influence the evolution of competition in retail financial markets.[136] Based on these findings, the FCA plans to continue monitoring big tech activities in financial services, both within and beyond the regulatory perimeter, to assess if policy changes are necessary to counteract competition harms.[137]
- **Review of organisational setting.** In 2022, the CFPB opened a new office, the Office of Competition and Innovation, replacing its Office of Innovation as part of a new approach to help spur innovation in financial services by promoting competition and identifying stumbling blocks for new market entrants.

Regulatory perimeter and oversight

85. **Following the entry and expansion of big techs in financial services, some authorities are considering how best to align their regulatory perimeter.** For example, in the UK respondents to a 2023 call for input suggested that the FCA would need to consider how its regulatory perimeter should evolve to address potential challenges with big techs operating at the boundary or outside the regulatory perimeter, which may include entering into partnerships. In response, the FCA announced a review of its supervisory approach towards big tech firms given they are active across different financial sectors with complementarities between them and with the big techs' core products and services.[138] The approach involves monitoring big tech activities both within and outside the regulatory perimeter, taking into account their business models, characteristics and cross-sectoral presence.[139]

86. **As financial groups become more complex and encompass a wider range of institutions, some regulators are expanding their oversight.** Traditionally, only bank-led groups received consolidated supervision, potentially leaving gaps in the oversight of non-bank financial groups, including those with non-bank lenders and payment institutions – unlike banks, these firms are supervised on a solo,

133 European Commission (2021).

134 European Commission (2023) and Knot (2024).

135 FCA (2023c).

136 These include the possibility of big techs exploiting their data from core digital services to strengthen their market position by raising barriers to entry or resorting to harmful price discrimination. Additionally, big tech platforms may become the primary interface through which customers do their banking, and therefore become gatekeepers in retail financial services. Lastly, the concentration of third-party services among a few big techs could limit the bargaining power of financial services firms regarding the terms of these back-end partnerships, which may also affect front-end partnerships.

137 The FCA also intends to identify and pilot use cases to empirically determine if big techs' data from their core digital activities are valuable in retail financial markets. If they are determined to be valuable, the FCA will explore how to align tech firms' incentives to encourage data-sharing where it benefits the entire data sharing ecosystem. The FCA and the PSR will also collaborate to understand the risks and opportunities associated with digital wallets (FCA (2024a)).

138 FCA (2023a).

139 FCA (2023c).

rather than consolidated, basis. Similarly, existing international frameworks for conglomerate supervision were designed before the rise of big techs and fintechs, and often only apply to groups with activities in specific sectors like banking or insurance. Against this background, some authorities have taken measures to extend the scope of group-wide supervision. For example:

- In the EU, the ESAs noted that some mixed activity-groups (MAGs), including big techs, do not have entities within their groups to which existing consolidation rules apply, and that these entities provide a range of financial services, including payments and lending.[140] Therefore, the ESAs recommended the European Commission consider: (i) the revision of existing consolidation rules and the creation of bespoke consolidation rules to ensure that the specific nature and inherent risks of MAGs carrying out financial services are adequately captured; and (ii) the creation of a structured regulatory and supervisory framework to extend to MAGs involved in financial services.[141] Similarly, the ECB recommended introducing more rigorous and comprehensive group-wide supervision for complex non-bank groups providing significant financial services akin to those offered by banks and surpassing certain thresholds, if such groups were found to operate in the EU.[142]
- In China, the PBC introduced measures to close perceived gaps in the regulation and supervision of firms that engage in two or more different types of financial services. Groups that exceed certain size thresholds are required by the PBC to create FHCs for all their financial activities and apply for an FHC licence. FHCs are regulated on a consolidated basis and subject to a range of requirements, including on ownership structure, governance and risk management, capital adequacy, related-party transactions, cross-subsidiary interactions, data governance, group structure and competition.[143]
- The Brazilian central bank aligned the prudential framework applicable to groups led by a payment institution with the one applicable to groups led by a financial institution (Box 4).

[140] They also noted that the identification of a financial conglomerate is predominantly focused on traditional bank-insurance (bancassurance) groups that meet certain thresholds in terms of size and significance of cross-sectoral activities, but does not capture emerging forms of diversified groups such as big techs. See Recommendations 7b and 7c in ESAs (2022).

[141] In addition, as part of the review of the second payments directive (PSD2), the EBA recommended that the European Commission introduce consolidated group supervision for payment and e-money institutions, potentially limited to "significant" institutions due to the challenges that come with consolidated supervision and the principle of proportionality(see EBA (2022a)).

[142] ECB (2024).

[143] See Annex 2 in Ehrentraud et al (2022) and Box 2 in Crisanto, Ehrentraud, Lawson and Restoy (2021) and Xuan (2023).

Box 4

Introducing "payment institution conglomerates" in Brazil

In recent years, the Central Bank of Brazil has aligned its prudential framework applicable to groups led by a payment institution (PI) with the one applicable to groups led by a financial institution. Before 2012, only banks were allowed to offer payments or issue credit cards in Brazil. This changed in 2013, when a new law (no 12.865) allowed tech firms and other non-banks to receive payment licences as payment institutions, subject to supervision on a solo level.

As the market evolved, many payment institutions began offering other financial services and establishing financial subsidiaries, particularly for lending. Since this new type of financial group was not subject to consolidated prudential requirements, concerns emerged that they operate like banking groups without being subject to similar rules.① For example, there was the potential for a payment institution's subsidiaries to transfer the credit risk of their lending activities back to the head payment institution, which was not required to hold capital against it. As such, subsidiaries of PI-led financial groups created incentives for excessive risk-taking.②

In response, in 2020, the Central Bank of Brazil proposed to extend regulatory requirements applicable to financial institution groups (called "financial institution conglomerates") to groups integrated by payment institutions.③ In 2022, new requirements were enacted which introduce a new typology of prudential conglomerate.④

	Revised typology for prudential conglomerates	
Type 1	Prudential conglomerate whose lead institution is a financial institution	Requirements unchanged
Type 2	Prudential conglomerate (i) whose lead institution is a payment institution; and (ii) which is *not* integrated by a financial institution	Type 2 conglomerates are subject to a simplified regulation aimed at maintaining the incentive for innovation and competition
Type 3	Prudential conglomerate (i) whose lead institution is a payment institution; and (ii) which is integrated by at least one financial institution	Type 3 conglomerates are subject to the segmentation of Brazilian financial system⑤

The new requirements make Type 2 and Type 3 conglomerates subject to prudential requirements on a consolidated level, as those applicable to financial institutions. They are intended to ensure the proportionate capture of all relevant risks and secure a level playing field between different types of financial group.⑥ They apply from July 2023, with full implementation in January 2025.⑦

Tech companies such as Mercado Libre and NuBank are now supervised as a Type 3 conglomerate (both are active in payments and credit) and therefore subject to the same rules as banks.

① One important difference is that these groups do not take deposits but issue e-money, which customers may perceive as deposit-like instruments. However, e-money reserves cannot be used for banking business as they need to be deposited with the central bank or invested in public debt. ② BCB (2022). ③ BCB Public Consultation Notice 78/2020, 11 November 2020. ④ BCB Resolutions nos 197, 198, 199, 200, 201 and 202. ⑤ As established by Resolution 4,553 of 30 January 2017. ⑥ BCB press release, 16 March 2022. ⑦ The reforms were initially intended to apply from 1 January 2023 but were deferred to 1 July 2023 (BCB Resolution 258).

87. **Digital wallets, often operating beyond the scope of regulatory oversight, have increasingly drawn regulators' attention.** While digital wallets that tokenise debit/credit cards may not fall within the regulatory perimeter, their growing importance has led some jurisdictions to review and clarify their regulatory treatment under existing obligations. Examples include the EU and the United Kingdom. Other jurisdictions, such as Australia and the US, are also proposing to bring digital wallets within the regulatory perimeter.

- In the EU, under the proposed PSD 3, "staged-wallets" (ie pre-paid digital wallets where users can store money for future online transaction) will be considered payment instruments and their providers subject to authorisation. In contrast, "pass-through wallets", involving the tokenisation of an existing payment instrument (eg credit card) will be considered as technical services and

therefore not subject to authorisation, as is already the case under PSD 2.[144] Nevertheless, digital wallets are subject to the Eurosystem oversight framework for electronic payment instruments, schemes and arrangements issued in November 2021.[145]

- In the UK, respondents to a call for input issued by the FCA in November 2023 requested that the FCA consider bringing large providers of digital wallets and payments apps into the existing regulatory perimeter of prudential and conduct regulation and supervision.[146] The FCA noted that, while the provision of digital wallet services is not in itself a regulated activity, they are becoming an increasingly important aspect of the UK payments landscape, and that it will work closely with the PSR to understand the risks and opportunities associated with digital wallets, launching a joint call for information specifically looking at digital wallets in July 2024.[147]
- The Australian government proposed rules that would enable the Reserve Bank of Australia (RBA) to monitor digital payments in the same way as credit card networks and other transactions. Specifically, the proposal would: (i) expand the definitions of "payment system" and "participant" to ensure the RBA has the ability to regulate new and emerging payment systems, such as digital wallet providers; and (ii) introduce a new ministerial designation power that will allow particular payment services or platforms that present risks of national significance to be subject to additional oversight by appropriate regulators.[148]
- In the US, efforts are ongoing to bring tech companies as providers of digital wallets and payment apps within the remit of consumer protection oversight. Specifically, in November 2023 the CFPB proposed to supervise large non-bank companies that offer services like digital wallets and payment apps (ie big techs and other technology firms handling more than 5 million transactions per year). The proposed rule would subject these firms to the CFPB's authority to conduct examinations and require them to: (i) comply with applicable federal consumer financial protection laws, including protections against unfair, deceptive and abusive acts and practices, rights of consumers transferring money and privacy rights; and (ii) play by the same rules as banks and credit unions.[149]

Further policy considerations

Addressing challenges from a more distributed value chain and front-end partnerships

88. **As responsibilities and risks are becoming dispersed among numerous entities within the value chain, the regulatory boundaries become increasingly blurred.** This poses novel challenges for day-to-day supervision due to the complexity and diversity of relationships and dependencies between banks and tech firms. This complexity not only amplifies the intricacy of oversight, but also hampers the supervisors' capacity to assess the risks stemming from a more distributed banking service delivery for both individual financial institutions and the entire financial system. In this context, in interviews conducted for this paper, supervisors highlighted the practical difficulties in gaining insight into the sometimes

144 This implies that a pass-through wallet operator is not categorised as a payment initiation service provider (Wagener (2024)). The status of pass-through wallets is proposed to be analysed as part of the PSD3 review clause.

145 This framework allows the ECB/Eurosystem to oversee businesses which support the use of payment cards, credit transfers, direct debits, e-money transfers and digital payment tokens, including digital wallets (see ECB (2021)).

146 Op cit.

147 FCA (2024a,b).

148 Australian Government (2023).

149 Through this supervisory authority, the CFPB intends to foster a level playing field between large tech companies and depository institutions in order to promote fair competition (see CFPB (2023)).

complex structure of partnership arrangements and the importance of ensuring that these arrangements do not infringe on consumer rights or impede effective supervision by authorities.

89. **The expansion of the value chain presents both micro- and macroprudential risks.** On a microprudential level, an expanded value chain not only heightens operational risks but also other types of risk that demand careful understanding and consideration by supervisors. Some of these risks, including those for banks' business model sustainability and financial soundness, may have received less attention so far but could gain importance over time. In addition, on a macroprudential level, an expanded value chain can create and distribute risk in unclear ways, potentially leading to a more interconnected financial system that increases the potential for spillover risks to materialise.[150]

90. **The more distributed the value chain becomes, the more practical challenges it presents for financial authorities.** This underscores the need for authorities to consider enhancing their training on partnership structures as they become more prevalent. These efforts should seek to ensure more innovative models are understood and relevant risks are appropriately addressed in day-to-day supervision. Relatedly, authorities may consider assessing the effectiveness of supervisory frameworks, which may result in updates to their on-site and off-site supervisory examination programmes.[151]

91. **Tech firms providing traditional banking services outside the banking regulatory perimeter may create an uneven playing field.** A tech firm may offer services such as deposit-taking, lending and payment processing through monoline licences or partnerships. Even though these services collectively resemble those of a traditional bank, they could be conducted outside the banking regulatory perimeter. This could potentially further disrupt the level playing field between tech firms and incumbent banks and, over time, dilute the value of holding a bank licence and therefore undermine the bank licensing regimes. Thus, maintaining a level playing field while supervising and enforcing the regulatory perimeter remains an ongoing challenge.

92. **Front-end partnerships should be given more consideration by policymakers.** To date, most focus has been on back-end partnerships, which is understandable given banks' significant reliance on tech firms for technology services. However, there are numerous front-end partnerships between banks and tech firms that are just beginning to attract the attention of authorities. This area may require more analytical work, coupled with strengthened engagement with tech firms, to better understand the risks and controls needed for different types of partnership, including the need for regulatory action. In interviews conducted for this paper, some banks and authorities felt that the risks associated with front-end partnerships, at this stage, might be best addressed by issuing specific requirements or additional supervisory guidance.

93. **The evolution of the banking value chain with the entry of new players necessitates regulatory and supervisory coordination across jurisdictions.** A more distributed value chain may cross jurisdictional boundaries between regulators within a country and internationally, given the frequently global business model of tech firms. Therefore, effective cooperation at both local and cross-border levels is essential. In particular, enhanced dialogue and novel forms of cooperation among financial authorities, competition commissions and data governance regulators are critical for improved institutional coordination. Big techs, in particular, present global challenges that can only be comprehensively addressed through a coordinated global response. To this end, further information-sharing across regulators is essential as they strive to better understand the implications of a more distributed value chain and partnership arrangements.

[150] Relatedly, see Hsu (2024).

[151] Along similar lines, McCaul (2024) argues that a "major restructuring is under way in financial services: integrating financial services into non-financial ecosystems, changing the risk landscape, blurring traditional industry lines and challenging conventional regulatory boundaries. Against this rapidly evolving backdrop, we also must continuously reassess the effectiveness of our supervisory framework".

Addressing challenges posed by big techs

94. **When considering partnerships, big techs present unique considerations when compared with fintechs.** The large scale of big techs, their negotiating power and banks' potentially limited capacity to effectively oversee and monitor their delivery of banking services can pose significant challenges. These challenges may also arise from potentially difficult to execute exit strategies, significant switching costs and limited substitutability of certain services. In interviews conducted for this paper, banks highlighted challenges with big techs being too large for banks to effectively monitor for third-party risk management purposes. They further indicated that these concerns applied to both back-end and front-end partnerships.

95. **The role of big techs in financial services could become even more significant if front-end partnerships become more prevalent.** Big techs already hold significant importance as providers of technology services, such as cloud services and, increasingly, AI. Their importance could grow even further if their involvement in front-end partnerships intensifies, solidifying their role as critical service providers to the financial market and irreplaceable managers of customer relationships. In this context, there is a case for supervisors to consider the potentially complex interplay between front- and back-end partnerships, underscoring the multifaceted role big techs play in the evolving digital landscape, and the potential for them to further consolidate their market dominance and therefore affect financial stability.

96. **The emergence of new corporate structures introduces risks that may not be sufficiently addressed by existing group-wide supervision frameworks.** Big techs (or large fintechs) often have multiple entities within their group that provide banking services through monoline licences and partnerships. These new forms of financial groups operate domestically and cross-border without any form of group-wide supervision, regardless of their significance. The lack of group-wide oversight, however, could lead to potential risks being overlooked, particularly those arising from interdependencies between various activities within the group.[152] At the current juncture, this scenario presents a unique challenge for regulatory authorities striving to maintain oversight and control in the rapidly evolving digital financial landscape.

97. **Specific entity-based rules for big tech operations in the financial sector could be warranted.** Big techs may offer banking services through a combination of partnerships and monoline licences. In terms of regulation, partnerships typically do not directly place requirements on the tech firm, and monoline licences are governed by sectoral regulations which typically follow an activity-based approach. However, as argued by Restoy (2022) and Carstens (2023), because a purely activity-based framework is ill suited to address the policy challenges associated with big techs, there is a need to directly regulate big techs by complementing sectoral regulations with group-wide entity-based requirements.[153]

98. **The application of entity-based rules for big techs should consider partnership arrangements.** These rules should only be applied to big techs that perform significant financial activities (big tech financial group (BTFGs)). Whether a big tech falls under this category should be based on the extent of its engagement in financial services. From a policy perspective, this could involve setting transparent thresholds that determine an entity's classification as a BTFG. Importantly, these thresholds should be designed to encompass big techs that offer financial products and services through partnerships without using their own balance sheet.[154]

[152] Crisanto et al (2022).

[153] In the context of big techs, risks emerge not only from the provision of a particular service, but also from the combination of all financial and non-financial activities they perform. This combination creates risks beyond the sum of those associated with each of the activities. See Ehrentraud et al (2022, 2024) and Restoy (2019).

[154] See Ehrentraud et al (2022).

Section 6 – Concluding remarks

99. **Innovation is a natural progression in any sector, including banking.** It can bring about new efficiencies, cost reductions and increased competitiveness and foster inclusion, but it necessitates careful consideration of its short- and long-term consequences. One such consequence is the impact bank-tech partnerships have on the banking value chain, and subsequently, the regulation and supervision of banking services.

100. **The evolution of tech firms in the banking sector, coupled with the growing complexity of their partnerships with banks, create challenges for regulators.** The continuous evolution and growth of front-end partnerships is blurring the lines between banking and non-financial activities and replacing the primarily direct relationships in banking with extended, intermediated chains of distinct services. Additionally, tech firms may utilise various subsidiaries within their groups to offer diverse financial services. These entities are often spread across multiple jurisdictions without consolidated oversight, resulting in limited visibility for regulators. Furthermore, when a tech firm offers or delivers services such as deposit-taking, lending and payments, this broadly resembles the functions of a traditional bank.

101. **In banking, maintaining public trust is a fundamental principle to ensure the stability of the banking system.** As non-bank entities like tech firms begin offering core banking services in innovative ways, grow their customer base and expand their market power, it remains essential for financial authorities to monitor the potential impact of these developments on public trust in the financial system and their ability to safeguard that trust. For this, authorities should consider the need to expand their tools and surveillance to prevent gaps in oversight.[155] Given the market share of more dominant tech firms and their potential for rapid expansion, a disruption in their financial service offerings could have significant implications for public trust and therefore financial stability. Therefore, additional actions at the national level, supported by international policy cooperation, could be warranted.

[155] See also McCaul (2024).

References

Apple Newsroom (2023): "Apple Card's savings account by Goldman Sachs reaches over $10 billion in deposits", 2 August.

Australian Government, the Treasury (2023): *Reforms to the Payment Systems (Regulation) Act 1998 – Exposure draft legislation*, November.

Austrian Banking Act (2024): *Bankwesengesetz (BWG)*, July.

Bank for International Settlements (2019): "Big tech in finance: opportunities and risks", *Annual Economic Report 2019*, Chapter III, June.

Barclays (2017): "From the archives: the ATM is 50", 27 June.

Basel Committee on Banking Supervision (BCBS) (2017): *Guidelines – Identification and management of step-in risk*, October.

——— (2018): *Sound practices – implications of fintech developments for banks and bank supervisors*, February.

——— (2019): *Report on open banking and application programming interfaces*, November.

——— (2021): *Newsletter on cyber security*, September.

——— (2023): *Supervisory newsletter on the adoption of POR and PSMOR*, November.

——— (2024a): *Core principles for effective banking supervision*, April.

——— (2024b): "Digitalisation of finance", *BCBS Working Papers*, May.

——— (2024c): "Literature review on financial technology and competition for banking services", *BCBS Working Papers*, June.

——— (2024d): *Principles for the sound management of third-party risk,* consultive document, July.

——— (2024e): *Core principles for effective banking supervision,* April.

BBVA (2023): "BBVA selects AWS to accelerate its data-driven transformation", 15 June.

Beck, T, L Gambacorta, Y Huang, Z Li and H Qiu (2022): "Big techs, QR code payments and financial inclusion", *BIS Working Papers*, no 1011, May.

Bian, W, L W Cong and Y Ji (2023): "The rise of e-wallets and buy-now-pay-later: Payment competition, credit expansion, and consumer behavior", *NBER Working Paper Series*, no 31202, May.

Board of Governors of the Federal Reserve System (2023): *Community bank access to innovation through partnerships*, October.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency (2024): *Joint statement on banks' arrangements with third parties to deliver bank deposit products and services*, July.

Borio, C, S Claessens and N Tarashev (2022): "Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs", *FSI Occasional Papers*, no 19.

Brainard, L (2017): "Where do banks fit in the fintech stack?", speech at the Northwestern Kellogg Public-Private Interface Conference on "New developments in consumer finance: research & practice", 28 April.

Carstens, A (2023): "Big techs in finance: forging a new regulatory path", remarks at the BIS conference on "Big techs in finance – implications for public policy", Basel, 8 February.

Central Bank of Brazil (BCB) (2022): *Financial Stability Report*, volume 21, no 2, November.

China Banking and Insurance Regulatory Commission (CBIRC) and People's Bank of China (PBC) (2021): *Circular of the General Office of the People's Bank of China on Regulating Commercial Banks' Personal Deposit Business through the Internet*, no 9, January.

Committee on Payments and Market Infrastructures (CPMI) (2022): *Improving access to payment systems for cross-border payments: best practices for self-assessments*, May.

Consumer Financial Protection Bureau (CFPB) (2022): "CFPB warns that digital marketing providers must comply with federal consumer finance protections", 10 August.

——— (2023): "CFPB proposes new federal oversight of big tech companies and other providers of digital wallets and payment apps", 7 November.

——— (2024): "CFPB takes action against Chime Financial for illegally delaying consumer refunds", 7 May.

Cornelli, G, J Frost, L Gambacorta, R Rau, R Wardrop and T Ziegler (2023): "Fintech and big tech credit: drivers of the growth of digital lending", *Journal of Banking & Finance*, 148:106742.

Crisanto, J C, C Donaldson, D Garcia Ocampo and J Prenio (2018): "Regulating and supervising the clouds: emerging prudential approaches for insurance companies", *FSI Insights on policy implementation*, no 13, December.

Crisanto, J C, J Ehrentraud and M Fabian (2021): "Big techs in finance: regulatory approaches and policy options", *FSI Briefs*, no 12, March.

Crisanto, J C, J Ehrentraud, A Lawson and F Restoy (2021): "Big tech regulation: what is going on?", *FSI Insights on policy implementation*, no 36, September.

Crisanto, J C, J Ehrentraud, M Fabian and A Monteil (2022): "Big tech interdependencies – a key policy blind spot", *FSI Insights on policy implementation*, no 44, July.

Croxson, K, J Frost, L Gambacorta and T Valletti (2022): "Platform-based business models and financial inclusion", *BIS Working Papers*, no 986, January.

Deutsche Bank (2020): "Deutsche Bank and Google Cloud sign pioneering cloud and innovation partnership", press release, 4 December.

Ehrentraud, J, D Garcia Ocampo and C Quevedo Vega (2020): "Regulating fintech financing: digital banks and fintech platforms", *FSI Insights on policy implementation*, no 27, August.

Ehrentraud, J, S Mure, E Noble and R Zamil (2024): "Safeguarding the financial system's spare tyre: regulating non-bank retail lenders in the digital era", *FSI Insights on policy implementation*, no 56, March.

Ehrentraud, J, J Prenio, C Boar, M Janfils and A Lawson (2021): "Fintech and payments: regulation digital payment services and e-money", *FSI Insights on policy implementation*, no 33, July.

Elias, J and H Son (2021): "Google abandons plans to offer bank accounts to users", CNBC, October.

European Banking Authority (EBA) (2017): *Final draft Regulatory Technical Standards on strong customer authentication and secure communication under PSD2*, 23 February.

——— (2018): *EBA report on the impact of fintech on incumbent credit institutions' business models*, July.

——— (2021): *Report on the use of digital platforms in the EU banking and payments sector*, September.

——— (2022a): *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, EBA/Op/2022/06, June.

——— (2022b): *Final report: Guidelines on the use of remote customer onboarding solutions under article 13(1) of Directive (EU) 2015/849*, EBA/GL/2022/15, November.

——— (2023): *Clarification of the relationship between EBA's Guidelines on outsourcing arrangements and Section 4 of the Directive (EU) 2015/849 – AML*, February.

——— (2024): *Final report on amending Guidelines on MLTF risk factors*, January.

European Central Bank (ECB) (2021): *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements*, November.

——— (2024): *Opinion of the European Central Bank of 30 April 2024 on a proposed regulation and directive on payment and electronic money services (CON/2024/13)*, April.

European Commission (2018): *Payment Services Directive: frequently asked questions*, January.

——— (2020): *Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014*, 24 September.

——— (2021): *A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, FISMA/2021/OP/0002.

——— (2023): *Modernising payment services and opening financial services data: new opportunities for consumers and businesses*, press release, June.

European Payments Council (EPC) (2024): "UPI: revolutionising real-time digital payments in India", *News and Insights*, June.

European Securities and Markets Authority (ESMA) (2024): *Cross sectoral work*.

European Supervisory Authorities (ESAs) (2022): *Joint European Supervisory Authority response to EC Call for Advice on digital finance*, ESA 2022 01, February.

FasterCapital (2024): *Magnetic stripe cards: a brief history and their modern relevance*, June.

Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System and Federal Deposit Insurance Corporation (collectively Federal Banking Agencies (FBA)) (2024a): *Joint statement on banks' arrangements with third parties to deliver bank deposit products and services*, July.

——— (2024b): *Request for information on bank-fintech arrangements involving banking products and services distributed to consumers and businesses*, July.

——— (2024c): *Third-party risk management: a guide for community banks*, May.

Federal Deposit Insurance Corporation (FDIC) (2024a): *Financial institution employee's guide to deposit insurance: pass-through deposit insurance coverage*, May.

——— (2024b): *FDIC official signs and advertising requirements, false advertising, misrepresentation of insured status, and misuse of the FDIC's name or logo*, January.

——— (2024c): "Recordkeeping requirements for custodial accounts", *Federal Register*, vol 89, no 191, October.

FDIC and Ohio Department of Commerce (2024): Consent order, FDIC-23-0110b, February.

Federal Register (2023): *Interagency guidance on third-party relationships: risk management*, June.

Feyen, E, J Frost, L Gambacorta, H Natarajan and M Saal (2021): "Fintech and the digital transformation of financial services: implications for market structure and public policy", *BIS Papers*, no 117, July.

Feyen, E, H Natarajan and M Saal (2023): *Fintech and the future of finance: market and policy implications*, World Bank, doi:10.1596/978-1-4648-1914-8.

Financial Conduct Authority (FCA) (2022a): "FCA warns Buy Now Pay Later firms about misleading adverts", press release, 19 August.

——— (2022b): "The potential competition impacts of Big Tech entry and expansion in retail financial services", *Discussion Paper 22/5*, October.

——— (2023a): "The potential competition impacts of Big Tech entry and expansion in retail financial services", *Feedback Statement 23/4*, July.

——— (2023b): *Primary credit brokers*, November.

——— (2023c): "Potential competition impacts from the data asymmetry between Big Tech firms and firms in financial services", *Call for Input*, November.

——— (2023d): "CP26/23 – Operational resilience: critical third parties to the UK financial sector", *Consultation paper 26/23 | FCA consultation paper 23/30*, December.

——— (2024a): "Potential competition impacts from the data asymmetry between Big Tech firms and firms in financial services", *Feedback Statement 24/1*, April.

——— (2024b): "Big tech and digital wallets", *Call for Information*, July.

Financial Stability Board (FSB) (2019a): *FinTech and market structure in financial services: Market developments and potential financial stability implications*, February.

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

——— (2019c): *Third-party dependencies in cloud services: Considerations on financial stability implications*, December.

——— (2020): *BigTech Firms in Finance in Emerging Market and Developing Economies: Market developments and potential financial stability implications*, October.

——— (2023): *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*, December.

Frost, J (2020): "The economic forces driving fintech adoption across countries", *BIS Working Papers*, no 838, February.

Frost J, L Gambacorta, Y Huang, H S Shin and P Zbinden (2019): "BigTech and the changing structure of financial intermediation", *BIS Working Paper*, no 779, April. Also published in *Economic Policy*, vol 34, no 100, pp 761–99.

Frost, J, L Gambacorta and H S Shin (2021): "From financial innovation to inclusion", *Finance & Development*, spring.

Gambacorta, L, Y Huang, Z Li, H Qiu and S Chen (2023): "Data versus collateral", *Review of Finance*, vol 27, no 2, March, pp 369–98.

Gambacorta, L, Y Huang, H Qiu and J Wang (2019): "How do machine learning and non-traditional data affect credit scoring? New evidence from a Chinese fintech firm", *BIS Working Papers*, no 834, December.

Gillis, A (2022): "Secure File Transfer Protocol (SSH File Transfer Protocol)", *TechTarget*, October.

Global Times (2021a): "China announces customer reserves management measure for non-bank payment institutions", 23 January.

——— (2021b): "New rules on online transactions unveiled at China's annual Consumer Rights Day gala", 16 March.

Hindu Bureau (2024): "Google Wallet vs Google Pay: understanding the key differences", *The Hindu*, May.

Hsu, M (2024): "Remarks before the Exchequer Club: size, complexity, and polarization in banking", 17 July.

ING Newsroom (2020): "ING in Germany and Amazon join forces in SME lending", 30 June.

European Supervisory Authorities (ESAs) (2024): *Report on 2023 stocktaking of BigTech direct financial services provision in the EU,* February.

Knot, K (2024): "Open finance regimes – experiences in some countries", speech at the Bank for International Settlements High Level Roundtable on Financial Inclusion, Basel, 12 March.

Koh, T Y and J Prenio (2023): "Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector", *FSI Insights on policy implementation*, no 53, November.

Liu, L, G Lu and W Xiong (2024): "The big tech lending model", January.

Luohan Academy Report (2019): *Digital technology and inclusive growth*, Shenzhen.

McCaul, E (2024): "Adapting to technological shifts: supervision in the evolving financial landscape", *The Eurofi Magazine*, September, p 97.

Office of the Comptroller of the Currency (OCC) (2021): "Payment systems", *Comptroller's Handbook*, version 1.0, October.

——— (2022): "Agreement by and between Blue Ridge Bank, National Association, Martinsville, Virginia and The Office of the Comptroller of the Currency, AA-NE-2022-43", August.

People's Bank of China (PBC) (2020): *Order No. 4 [2020] of the People's Bank of China – Trial measures on regulation of financial holding companies*, 11 September.

——— (2021): *Regulations on non-bank payment institutions (draft for comments)*, 21 January.

Reserve Bank of India (RBI) (2020): *Guidelines on regulation of payment aggregators and payment gateways*, RBI/DPSS/2019-20/174, March.

——— (2021): *Report of the Working Group on Digital Lending Including Lending through Online Platforms and Mobile Apps*, November.

——— (2022): *Guidelines on Digital Lending*, RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23, September.

——— (2023): *Master direction on outsourcing of information technology services*, RBI/2023-24/102, April.

——— (2024): *Guidance Note on Operational Risk Management and Operational Resilience*, RBI/2024-25/31, April.

Restoy, F (2017): "Fintech regulation: how to achieve a level playing field", *FSI Occasional Papers*, no 17, February.

——— (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.

——— (2021): "Regulating fintech: is an activity-based approach the solution?", speech to the fintech working group at the European Parliament, 16 June.

Santander (2024): "Santander and Amazon launch their new credit card Amazon Visa in Germany which rewards customers for purchases at no annual fee", press release, 12 August.

Staples, A (2024): "Apple seeks to end its credit card and savings account partnership with Goldman Sachs", *CNBC Select*, 17 October.

Stipano, D, K Howell and C Wilson (2023): Anti-money laundering / countering the financing of terrorism: the opportunities and challenges of bank-fintech partnerships, *ABA Bank Compliance*, May/June (2023).

US Department of the Treasury (2022): *Assessing the impact of new entrant non-bank firms in competition in consumer finance markets*, Report to the White House Competition Council, November.

Wagener, K (2024): "PSR/PSD 3: The digital purse – the 'wallet'",25 April.

Xuan, C (2023): "Evolving regulatory and supervisory architecture to oversee big techs", remarks at the BIS conference "Big techs in finance – implications for public policy", Basel, February.

Zamil, R and A Lawson (2022): "Gatekeeping the gatekeepers: when bigtechs and fintechs own banks-benefits, risks and policy options", *FSI Insights on policy implementation*, no 39, January.

Annex: selected bank-tech partnerships

Tech firms	BT/RG/FT	No of users[2]	Bank offering	Product	Bank partner	Jurisdiction
Apple	BT	1 billion iPhone users	Deposits	Savings account	Goldman Sachs Bank	United States
			Payments	Prepaid cards	Green Dot Bank	United States
			Payments	Digital wallet services	Global Bank Partners	Global
BukaTabungan	RG	Over 110 million users and 20 million business owners	Deposits	Deposit-taking	Standard Chartered Bank	Indonesia
Amazon	BT	200 million Prime members	Credit	SME lending	ING	European Union
			Credit	Consumer credit referral	Barclays	United Kingdom
			Credit	SME credit referral	Goldman Sachs Bank	United States
Ant Group (incl AliPay)	BT	1.3 billion annual active consumer on e-commerce platforms	Payments	Class I operation of stored-value accounts, Class II operation of stored-value accounts[1], Class I processing of payment transactions	Numerous bank partners	China
			Credit	Consumer & SME Lending	Numerous bank partners	China
Atome	FT	30 million	Credit	Consumer lending	Standard Chartered Bank	Singapore Malaysia
Chime	FT	Over 14.5 million users	Deposits	Checking accounts	Bancorp Bank and Stride Bank	United States
Freo	FT	1.5 million customers	Deposits	Savings account	Equitas Small Finance Bank	India
Google	BT	2 billion monthly active devices running Android	Payments	Digital wallet services	Global bank partners	Global
			Credit	SME lending	Numerous bank partners	India
Indifi	FT	Unavailable	Credit	SME lending	Numerous bank partners	India
Kontist	FT	Over 50,000 customers	Deposit	Business account	Solaris Bank	European Union
PayPal	FT	428 million active accounts	Deposits & payments	Deposit-taking & payment services	Several bank partners	United States
			Credit	Business loans	WebBank	United States
Samsung	BT	1 billion users	Deposits	Cash management account	SoFi Bank	United States
			Payments	Digital wallet services	Global bank partners	Global
Tide	FT	500,000 members	Deposits	Business account	ClearBank	United Kingdom
			Credit	Business loans	British Business Bank	United Kingdom
Tomorrow	FT	Over 120,000	Deposits	Bank accounts	Solaris Bank	Germany

[1] Limited to online real-name payment account top-ups. Sorted alphabetically. [2] "No of users" represents the broader international user base outside of the specific jurisdictions mentioned in partnerships. Sources: Annual reports, public articles, FSI analyses.