Unchained

Supervision in an open banking sector

DeNederlandscheBank

EUROSYSTEEM

Contents

1 Introduction

The banking sector is becoming more open. Driven by developments such as technological innovation and changing regulations, new parties are entering the financial sector. This means a shifting playing field for incumbents. They no longer serve the entire value chain – from product development to end customer. Various parties are taking up positions in the value chain, and are collaborating in different ways with traditional banks.

In this publication, De Nederlandsche Bank (DNB) assesses the consequences of a more open banking sector for prudential and integrity supervision. This ties in with one of the key priorities in our Supervisory Strategy 2018-2022: "Responding to technological innovation".

DNB sees advantages in the unbundling of value chains and a more open sector as this will allow innovation to blossom and will increase the efficiency of financial services. At the same time, DNB considers it crucial that this openness does not lead to lack of clarity about responsibility. Even in more open, longer and sometimes more complex chains, supervised institutions – and their boards – are still responsible. They are responsible for their products and services to customers even if they outsource parts of this or collaborate with third parties.

The following section describes the various ways in which the sector is opening up. Section 3 sets out the consequences for banks of an open banking sector, focusing respectively on operational management, integrity risk management and business models. Section 4 addresses the consequences for the financial system as a whole, highlighting both the opportunities and the risks. The final section deals with expectations regarding the sector and the next steps for our supervision.

2 The open banking sector

2.1 Openness of the value chain

The banking sector is opening up.[1] The sector is opening on two fronts, in value chains (vertically), and customer interaction (horizontally).

Banks are unbundling their value chains (vertically). Banking value chains comprise different processes, ranging from back-office support and product development to customer sales. Banks do not necessarily carry out all activities in the value chain. Instead, third parties are taking up roles in the value chain, such as through IT infrastructure outsourcing. Banks are also collaborating with third parties to develop new and innovative services.

Banks are no longer the obvious party to manage client interactions (horizontal). Customers are no longer reliant on their own bank as they can now get an overview of all their accounts at different banks with apps from just one party. Customer interaction also fades into the background if platforms get a foothold in banking. These virtual markets will connect consumers (demand side) with producers (supply side). Some banks are taking steps to offer their services alongside competing services from third parties via platforms in the future. Figure 1 presents a stylised view of bank lending in terms of vertical unbundling and horizontal shifts in customer contact.

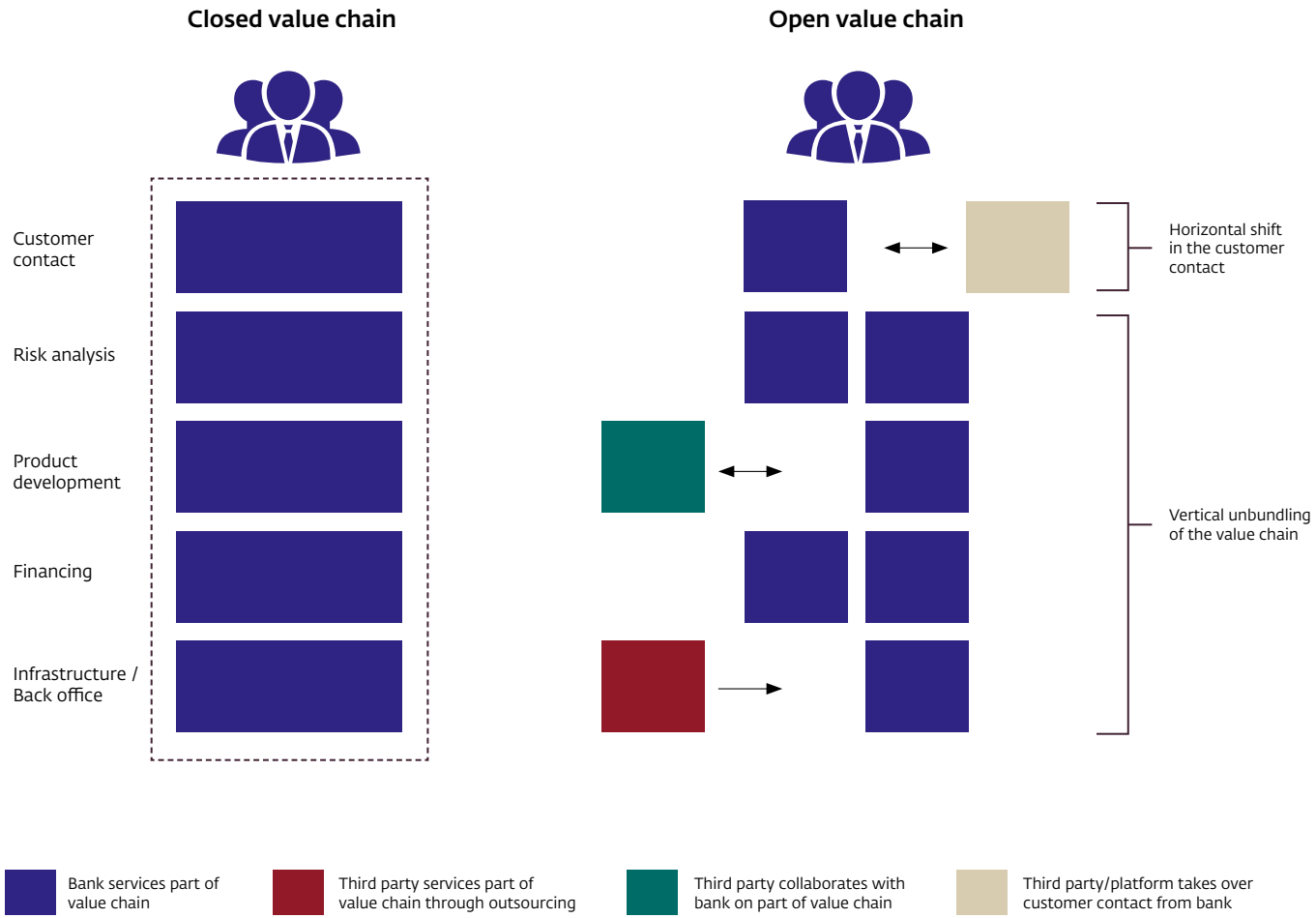
2.2 Openness via outsourcing

Outsourcing is becoming increasingly essential for banking operations. An ECB study revealed that European banks spend roughly 42% of their IT budgets on outsourcing to third parties, compared to 35% five years ago. Whereas outsourcing initially concerned only supporting services such as HR administration and marketing activities, nowadays material activities closer to the core business are also being outsourced. This has partly been made possible by new types of outsourcing operations which are on the rise thanks to technological advances. Below we look at two relatively new forms of outsourcing, namely Banking-as-a-Service, and cloud computing.

Banking-as-a-Service involves parties offering banking infrastructure to banks and non-banks. In this way, banks no longer have to maintain all the systems themselves but can use third party products. In the Netherlands there are examples of banks that outsource payment services in this manner. Another example of Banking-as-a-Service is loan origination through white labelling.[2] If this service is obtained by non-banks, then they use both the licence held by the white label provider as well as the underlying infrastructure.

1 We define an open banking sector as one in which the value chain is open, and is not the exclusive preserve of a single entity, in this case the bank. Various parties are entering the chain, and we see the introduction of the revised Payment Services Directive (PSD2) as one of the catalysts of this more open banking sector. Our definition is therefore broader than the term "open banking" as used in the United Kingdom and which refers to banks' obligations to share transaction data with third parties under certain conditions.
2 The provision of this service is seen as outsourcing.

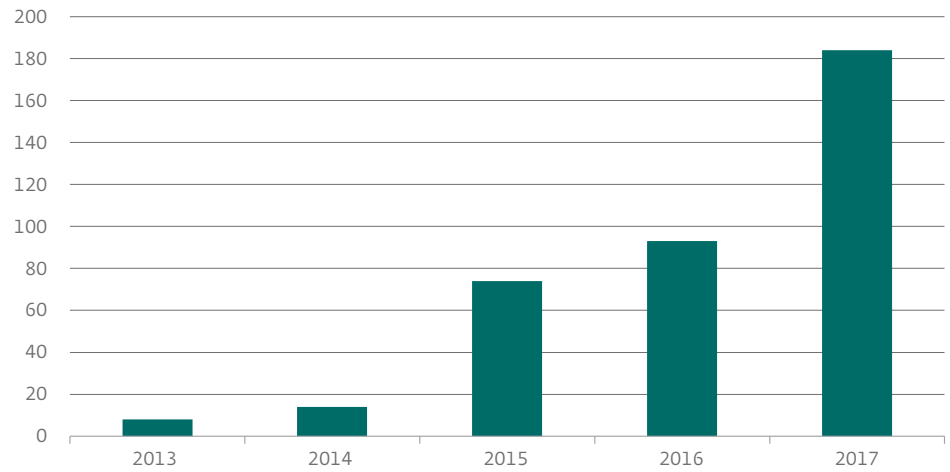
Figure 1 Openness in the bank lending value chain (stylised)



Another increasingly important form of outsourcing is cloud computing. The number of cloud computing outsourcing agreements reported to DNB increased to more than 180 in the four years prior to 2017 (see Figure 2).[3] Cloud computing provides a relatively quick and simple way to adjust computing or processing power. It also means banks need to manage and maintain less in-house server and computer capacity. Banks can outsource various IT services to the cloud, from supporting infrastructure such as servers and storage capacity (Infrastructure-as-a-Service), to software applications such as email (Software-as-a-Service). In the near future, banks are expected to also start using the cloud for more critical tasks, such as credit scoring.[4]

Figure 2 Rapid increase in cloud outsourcing operations

Number of cloud outsourcing operations reported by banks in the Netherlands



Source: DNB

3 The population comprises 23 banks based in the Netherlands.
4 PwC (2016), "Financial Services Technology 2020 and Beyond: Embracing Disruption."

2.3 Openness via partnerships

Banks and new FinTech parties can benefit from each other's strong points through partnerships. Banks are primarily interested in FinTech's technological expertise (see box 1). Whereas five years ago there was no or little mention of collaboration with FinTech parties, the three major banks in the Netherlands have now reported over 250 partnerships. Over 90% of European banks collaborate with FinTechs.[5] Contracts with banks appeal to FinTechs as it gives them access to customer bases and data, more opportunities to attract financing, and experience in how to comply with regulatory and legislative requirements. Globally, three quarters of FinTech companies prioritise cooperation with established banks.[6] We distinguish two different approaches towards partnerships. In the first approach banks themselves take the initiative and allocate time or budget, such as acquiring holdings in FinTech companies. In the second approach towards partnerships banks create the preconditions, but leave it up to other parties to take the initiative. One example of such partnerships are developer portals. These are online environments where app and software developers use the banking infrastructure to build new applications.

Box 1 Artificial intelligence applications in the banking system

Banks are increasingly using artificial intelligence applications (AI). A more open banking sector amplifies this trend. Banks often develop AI applications in partnership with FinTech, or obtain them through outsourcing.[7] AI engages with the development of computer systems capable of performing tasks that traditionally require human intelligence.[8] Banks already use AI to interact with customers via, for example, voice-activated banking and availability of a 24-hour virtual workforce (chatbots). Furthermore, with the help of machine learning, advanced risk analyses can be conducted for automated investment advice, or lending to small and medium-sized enterprises. Machine learning can also be used to support risk models by identifying patterns in large datasets. This form of 'learning' can either be (semi-)supervised, or unsupervised.[9] In both cases, the decisions made must be traceable and explainable, as described in section 5.

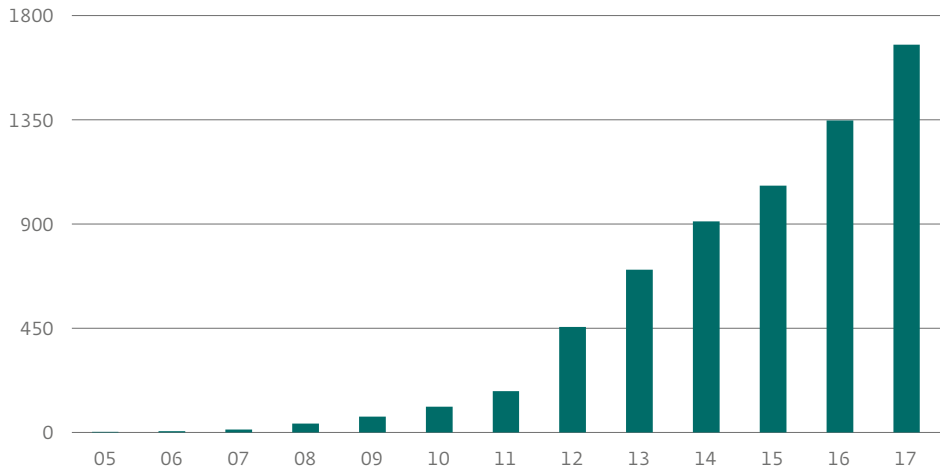
5 EBA (2018), "Report on the impact of incumbent credit institution's business models".
6 Capgemini (2017), "The World FinTech Report 2017".
7 Bafin (2018), "Big data meets artificial intelligence. Challenges and implications for the supervision of and regulation of financial services".
8 FSB (2017), "Artificial intelligence and machine learning in financial services: Market developments and financial stability implications".
9 In the case of supervised machine learning, a model learns the outcomes it needs to provide, based on data in a labelled dataset. All elements in a labelled dataset have a label, and therefore belong to a particular category. The outcomes are predetermined. In the case of unsupervised learning, it is left up to the models to discover and classify the data themselves. The model makes conclusions based on an unlabelled dataset. The outcomes are therefore not known in advance. Semi-supervised learning is a combination of the two techniques described above.

Banks collaborate with FinTech companies through shareholdings and other investment contracts. Banks can set up joint ventures with a third party and then divide responsibility and risk/profit according to predetermined agreements. Banks also participate in FinTech firms through their venture capital funds. The three major banks in the Netherlands have earmarked a total of approximately EUR 420 million for this purpose. Investments made through these venture capital funds are intended to generate know-how, which the bank can then use for its own business. However, there are also looser contractual relationships. For example, several international banks are cooperating on cross-border payment systems based on blockchain technology.

Through developer portals, banks can also facilitate cooperation with FinTech firms. Banks can open up their infrastructure via application programming interfaces (APIs). An API is a connection point that allows computer applications to communicate with each other and to exchange information (data) over a network. By making APIs externally available, banks are able to give third parties controlled access to part of their infrastructure and data.[10] Banks have already been using APIs internally for some time. The number of publicly available APIs by banks is estimated to have grown significantly in recent years. (see Figure 3). Various European banks have developer portals, where APIs can be used to develop new applications for banking services, such as adding payment options to accounting software for businesses.

Figure 3 Use of APIs in the financial sector is increasing

Number of public APIs in the international financial sector



Source: Accenture

10 This is different to *screen scraping*, where a third party can gain access to a customer's bank account using the customer's login details.

2.4 Openness via customer contact

The banking sector is becoming increasingly open as banks are obliged to share payment data with third parties if customers give their consent. This is a result of the revised Payment Services Directive (PSD2), which enters into force in 2019. Under PSD2, consumers can initiate payments or view their account information without needing direct contact with their bank. New parties such as account information service providers and payment initiation services will then interact with customers.[11] We commissioned a survey to gauge the extent to which consumers are willing to share their payment data with third parties (see box 2).

Several banks are also taking steps to arrange future customer contact through a platform for financial services. Entering into partnerships with the various parties marks the first step towards distributing complementary services and products through a platform. There are varying definitions of what a platform is.[12] They typically involve matching supply and demand by bringing together consumers and producers of products and services, and therefore lowering transaction costs for the users of the platform. A defining attribute of a platform are its network effects, which means that as the number of users on a platform increases, the added value for an individual user also increases. Finally, a distribution platform is able to respond to individual needs of users based on data analysis. Several European banks have expressed the ambition to develop into financial platforms that offer customers third party services, including those provided by their competitors.

Banks can take on the role of a platform supplier or become platform providers, with varying consequences for customer contact. As suppliers, banks distribute their products and services on platforms provided by other financial institutions, or possibly by bigtechs in the future. The platform would in this case constitute another distribution channel for banks. As platform providers, banks would manage their own platform and maintain customer relations. In this case, banks would not only have to ensure that all transactions on the platform are conducted smoothly, but also have responsibility for maintaining trust between suppliers and consumers by guaranteeing the quality of the products offered. One of the core tasks for platform provider banks is therefore due diligence and management of the suppliers active on the platform.[13] A major question facing banks is whether they will manage these platforms themselves or whether bigtechs will assume this role. The two bigtechs in Asia - Alipay and Tencent - have in a relatively short time managed to take over 93% of the mobile payments market.[14] Bigtechs in the western world such as Amazon and Facebook have also recently started offering payment services on their platforms, and are taking preliminary steps to get involved in other banking activities, often in partnership with banks.

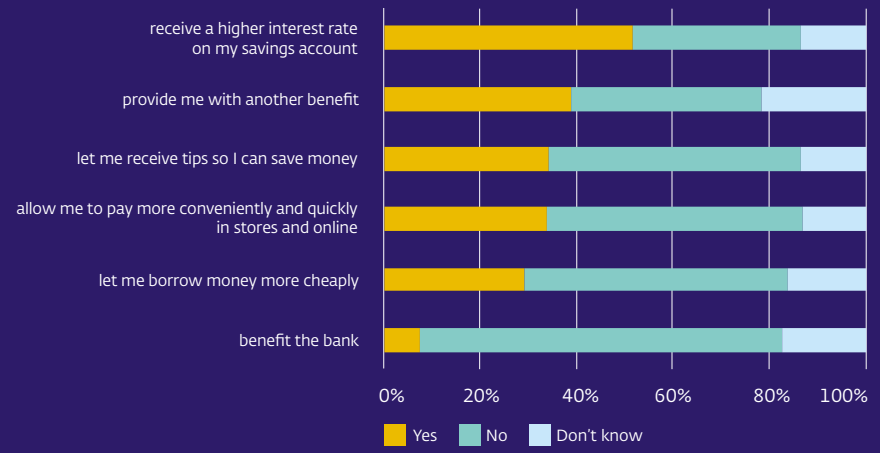
11 Provided these service providers are under DNB's supervision.
12 We focus here on distribution platforms, or platforms that are oriented towards customer contact (the front end of the value chain). There are also product platforms, such as banks' open API platforms through which new products are developed in the middle of the value chain (see above).
13 In practice, a bank that manages its own platform can offer its products on another platform.
14 Financial Times (2018), "Tencent and Alipay set to lose $1bn in revenue from payment rules". 15 July 2018. These two Asian bigtechs have steadily expanded their platforms by offering other banking services, such as loans and asset management.

Box 2 How willing are Dutch consumers to share their data?

It is not certain whether account holders will be inclined to share their data after the introduction of PSD2. We conducted a survey in cooperation with CenterData to gauge how willing consumers are to share their payment data, and what considerations play a role in this respect. Around 65% of households indicated that they would rather give their consent for a bank to use their payment data, instead of a tech company. This willingness to share data seems to be further dependent on the benefits households receive in return (see Figure 4). Account holders appear to be most interested if they receive a higher savings rate in exchange for their data (52%). This percentage increases the younger the account holders are.

Figure 4 Consumers want to see benefits for sharing their payment data

I give consent to my bank to use my payment data if the purpose is to...



Source: DNB

3 Consequences for financial institutions

An open banking sector has consequences for individual banks. In this section we will discuss how the unbundling of value chains affects operational risks, integrity risks, and lastly business models.

3.1 Consequences for operational risk

An open banking sector offers opportunities to improve operational processes and reduce risk. The quality and cost-efficiency of operational processes improves if banks collaborate with specialized technology companies which can carry out certain tasks more effectively and at a lower cost, such as cybersecurity. At the same time, collaboration with third parties gives banks the opportunity to focus on their core tasks. Lastly, the use of for example cloud services provides greater operational flexibility.

The type of operational risk changes due to a shift from internal risks towards third party vendor risks.[15] If the value chain consists of a series of independent parties, then it becomes more difficult for banks to have insight into how responsibilities are assigned between the parties, or to determine if these parties have adequate risk management. Risk management becomes more complex as core processes are carried out by multiple third parties, or if service providers also subcontract certain operations to other third parties themselves. Subcontracting results in longer and more complex value chains, and therefore hampers operational risk management. It is thus important that institutions address this issue in their operational risk management framework, as discussed further in section 5. In several countries, third-party service providers are under direct financial supervision (see box 3).

The type of operational risk is also changing due to the use of complex technologies. Knowledge asymmetry with third parties increases as technological knowledge becomes more specialised. Technologies such as near field communication, biometrics, cloud computing or machine learning are typical IT fields, which are increasingly applied within the banking sector and require specialist competencies to be properly applied and assessed. As knowledge asymmetry increases, it requires additional effort on the part of banks to maintain effective oversight and have sufficient knowledge of underlying technologies. Risks that result from the application of advanced technologies by third parties should also be adequately incorporated in banks' operational risk management.

Lastly, the relative importance of operational risk increases due to more intensive use of data and the interconnectedness of parties through the internet. In an open banking sector, third parties have access to banks' sensitive data, which requires banks to have sufficient insight into which data they share and whether third parties have adequate data security measures

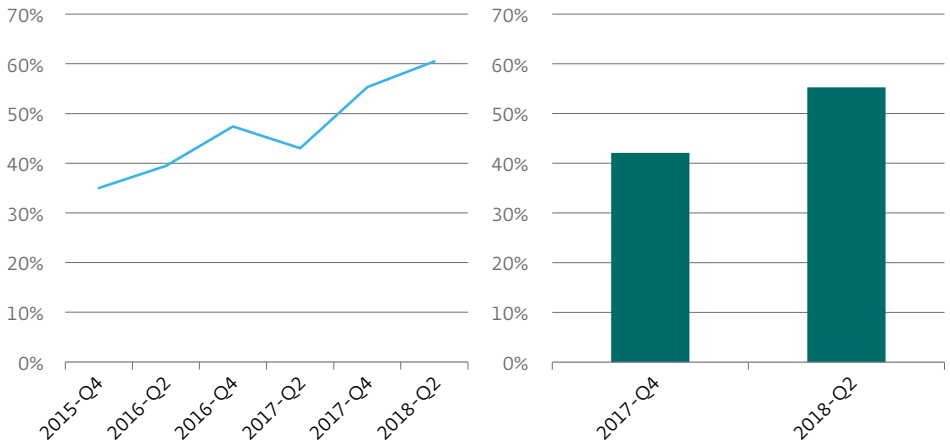
15 Vendor risks relate to the risks associated with outsourced service providers, which can for example include delivery problems, data breaches or even bankruptcy. BCBS defines operational risk as all risks of losses arising as a result of human activity, inadequate internal processes, as well as risks caused by external events. See: BCBS (2011), "Principles for the sound management of operational risk".

in place. Statutory requirements on data use and protection have been tightened under the General Data Protection Regulation (GDPR). Infringements of the GDPR can result in fines being imposed – of up to 4% of annual business revenues – which could potentially affect a bank's solvency. Data security is therefore directly (through operational risk), as well as indirectly (through fines) relevant for prudential supervision. In the area of data security and cyber risk, banks are subject to supervision from several supervisory authorities.[16]

Dutch and European banks themselves also recognise the increasing importance of operational risk and the role of data security in this respect (see figure 5).

Figure 5 Banks have seen an increase in operational risk and the importance of data security

Percentage of European banks that have seen an increase in operational risk (left) and percentage of European banks that consider cyber risk and data security to be a key driver of this (right)



Source: DNB, EBA Risk Assessment Survey

16 Including the Dutch Data Protection Authority, Dutch Radiocommunications Agency, the Authority for Consumers & Markets and DNB.

Box 3: Supervising third parties – the scope of supervision

In a number of jurisdictions financial supervisory authorities also have the possibility to conduct direct supervision of third parties. In the United States it is in the remit of federal supervisory authorities to conduct inspections at third parties.[17] They have developed a specific oversight framework under which they jointly supervise both systemic as well as regional technology service providers (TSP). These inspections mainly focus on IT and operational risks.

In Luxembourg there is a licensing obligation for third parties that supply specific services to financial institutions, which are known as professionals of the financial sector (PFS). These include key supporting services such as administration or IT services, but not cloud providers. PFS-licensed companies fall under the direct supervision of the national supervisor, the Commission de Surveillance du Sector Financier (CSSF). In this case, as in the United States, financial institutions retain ultimate responsibility for risk management.

DNB does not directly supervise third parties that carry out activities for financial institutions. Under EU law, banks remain responsible for the activities they outsource. Furthermore outsourcing contracts must stipulate that the supervisory authority is able to gain full access to all information and also has the possibility to conduct on-site examinations (access, information and audit right). DNB also scrutinises contracts to ensure they include this audit right so inspections can be effectively conducted at third parties, if necessary from a risk perspective.

3.2 Consequences for integrity risks

Management of integrity risks could improve in an open banking sector. Banks may for example cooperate in the area of know-your-customer research or the monitoring of suspicious transactions. This may lead to more insights and help prevent financial-economic crime. In the Netherlands banks are exploring the possibility of setting up a private central unit to carry out know-your-customer research. Although such an initiative would require overcoming numerous practical and legal barriers, including concerning the ownership of the unit, data and information, it may also result in more effective and efficient checks. A similar sort of private partnership is conceivable in the area of transaction monitoring.

Banks may become less effective in their role as gatekeepers as the number of links in the value chain multiply. Customer due diligence can become a separate link itself through outsourcing. A DNB survey shows that approximately 20% of the banks in the Netherlands outsource part of their customer due diligence process. This primarily concerns customer acceptance, as third parties are able to offer a more user-friendly experience for onboarding new account holders. It is pivotal that this does not lower the quality of customer screening. The effectiveness of the gatekeeper-role could also be undermined when banks expand their range of services through APIs to include services that may facilitate financial crime.[18] Take for example cryptos, which make it more difficult to trace the original source of

17 The Federal supervisory authorities are the Board of Governors of the Federal Reverse System (FRB), the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC). For relevant legislation see the Bank Service Company Act, 12 USC §1867(c).
18 New online-only banks in Europe currently offer these services through third parties.

income. For the integrity of the financial system as a whole it is important that providers of for example crypto wallets and crypto exchange platforms are subject to the same requirements for preventing financial crime as financial institutions are. Crypto services will be subject to these requirements as of January 2020.[19]

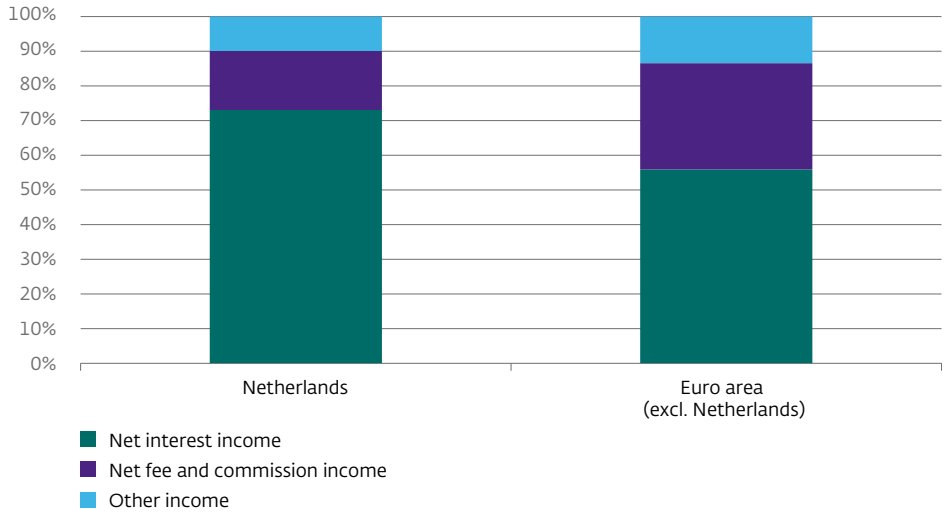
3.3 Consequences for business models

An open banking sector offers opportunities for diversification of a bank's business model. Through the use of APIs banks can offer new products such as programmes to digitally establish customer identities, market analysis or invoicing services. There are also – mainly new – banks that offer their banking infrastructure (Banking-as-a-Service). These innovations typically generate revenue on transaction, subscription or licensing fees rather than interest rate margins.

For Dutch banks, this may lower their relative dependence on net interest income (see Figure 6).

An open banking sector can squeeze profit margins if openness leads to greater competition due to the entry of new players. New parties such as data aggregators make it easier to compare and switch between different providers, which could ultimately increase the interest rate sensitivity of deposits. This effect of course depends on the extent to which consumers are willing to use these services offered by new players and grant permission to third parties to retrieve data.[20] Even if these data aggregators do not in practice lead to more switching, they could result in additional pressure on prices through increased transparency. For example, if as a result of greater price transparency Dutch banks would have to pay an additional 25 basis points on deposits, interest expenses would

Figure 6 Composition of banks' net operating income



Source: DNB, ECB (2017)

3.1 Consequences for operational risk
3.2 Consequences for integrity risk
3.3 Consequences for business models

19 This is provided for in the Fifth Anti-Money Laundering Directive, which will apply to Member States when it enters into force on 10 January 2020.
20 A 2014 survey by the ACM shows for example that 73% of Dutch people over the age of 18 have never switched bank. See: ACM (2014), "Barrières voor toetreding tot de Nederlandse bancaire retailsector".

according to calculations ceteris paribus increase by EUR 830 million, an amount equal to 5.5% of total pre-tax earnings.[21]

In the longer term, profit margins may come under pressure as banks lose the primary contact with customers, and in so doing also lose opportunities to sell other products to the same customer (cross-selling).[22] An open banking sector can change the relationship between the customer and the bank. While account holders traditionally required contact with their bank for all transactions, as a result of internet applications such as PayPal or mobile payments, this is less and less the case. With the advent of mobile wallets, banks are becoming consigned to the background. Furthermore, payment initiation services are appearing on the market, which could also replace the direct contact between bank and customer.

Finally, the bank's role in the value chain determines whether the bank maintains the primary customer contact, which has consequences for the bank's business model. This role partly depends on the extent and rate of platformification of the sector.

21 The difference between the most favourable and least favourable interest rates in the savings market amounts to 25 basis points.
22 PwC (2016), "How bankers can become innovation leaders again." PwC analyses have shown that opportunities for cross-selling can be three times higher in the case of clients with a current account than in the case of clients without a current account. Savings accounts are also an example of cross-selling products.

4 Consequences for the financial system

In addition to consequences for individual financial institutions, an open banking sector also has implications for the stability of the financial system as a whole. In this section we will first look at the opportunities for the financial system before discussing the risks that unbundling of the value chain may entail.

4.1 Opportunities for the financial system

The entry of new parties to the value chain contributes to greater efficiency of services and diversity in the financial sector. Firstly, an open banking sector will ensure greater competition and price transparency. Furthermore, new parties are able to offer their services more efficiently thanks to fully digital business models and use of the latest technologies. The newcomers stimulate incumbent banks to invest in modernising their services. This can lead to lower margins on financial products, which translates into lower prices for the consumer. Secondly, there will be less dependence on a small group of financial institutions as several other parties would now be able to offer the same services. The financial system as a whole will therefore become less vulnerable.

An open banking sector has consequences for banks' resolvability. As different components in the chain are easier to (dis)connect via plug-and-play systems, it is only the core of the bank, and not the entire bank that needs to be placed in resolution. However, the increasing complexity of collaborations and outsourcing makes it more difficult to see which parties are responsible for which activities. It is therefore important that banks do not include conditions in service level agreements with third parties that may impede resolution.

4.2 Risks for the financial system

Sector and cross-border interconnectedness between parties increases in an open banking sector. IT connections among banks and between banks and tech companies may increase, which heightens the risk of contagion in the event of operational disruption. The level of interdependence in the sector may also increase in due course, as several incumbent banks are working on activities beyond the traditional banking sector. This is referred to in the sector as "beyond banking". Banks may for example also offer brokerage services in combination with their own financial products. This mixing with other sectors offers opportunities for more diversified streams of revenue, but can also expose individual institutions to reputational risks. Lastly, the combination of a digital business model and a European passport makes it relatively easy to offer banking services in several countries. A payment institution can for example, on the basis of a licence from one European authority, also provide services to other European countries without actively being under supervision there.

Risks may shift onto new parties which do not have to comply with the same, or similar, regulations as existing financial institutions. New parties are entering the value chain which do not have a background in the financial sector or familiarity with its regulation. These parties may not manage certain risks as well because they for example use models that have not yet undergone a full credit cycle. Take for example credit risk models with self-learning algorithms, often

4.1 Opportunities for the financial system
4.2 Risks for the financial system

used by online marketplace lenders which have yet to demonstrate whether their predictive power is adequate in a recession. [23] Another example is in the area of cyber risks. European supervisors work together on the cyber resilience of the financial sector through red teaming programs (ethical hacking). This supervisory approach may become less effective if banks transfer their IT processes to parties that do not have to cooperate in this area, resulting in incomplete or not up to date insights into cyber risks.

Outsourcing and subcontracting can lead to the build-up of concentration risks if banks use the same service providers. An individual bank does not have insight into potential concentration risks at sector level, and takes service providers into consideration based on the advantages they offer for its own business operations. These service providers may therefore create a single point of failure, which can lead to the failure of crucial services such as payment transactions at systemic level. This not only endangers the business continuity of individual institutions, but can also undermine confidence in the banking sector. For example concentration in the cloud services sector is increasing, with four large providers accounting for 60% of the global market.[24] Subcontracting can further amplify potential concentration risks. Parties to which banks outsource may in turn employ the same service providers. In practice, FinTechs also use international cloud service providers and data centres.

23 Stijn Claessens, Jon Frost, Grant Turner, Feng Zhu (2018), "Fintech credit markets around the world: size, drivers and policy issues", BIS Quarterly Review, September.
24 Synergy Research Group (2017), "Cloud Market Keeps Growing at Over 40%; Amazon Still Increases its Share," October. This concerns the entire market for cloud services, not just financial institutions.

4.1 Opportunities for the financial system
4.2 Risks for the financial system

5 Focal points and next steps

DNB considers innovation essential for a long-term viable banking sector. However, innovation also involves risks. DNB wants to inform the sector in a timely and clear manner about the supervisory expectations in this respect. The aim is to ensure good preconditions for innovation, and to reduce the impact of potential incidents in an open banking sector. Effective supervision is not static, but requires continuous response to changes in the financial sector. We therefore want to continue the dialogue with market parties to ensure supervision does not unnecessarily inhibit innovation. Initiatives such as the InnovationHub, and the regulatory sandbox can contribute in this respect.

5.1 Focal points for the banking sector

Banks retain responsibility for managing the risks associated with outsourced activities. The Financial Supervision Act (*Wet op het financieel toezicht – Wft*) allows banks to conditionally outsource certain activities. This means that banks must have adequate policy, procedures and measures in place to manage outsourcing. Also outsourcing arrangements must never impair DNB supervision. DNB is currently working with the European Banking Authority (EBA) to tighten outsourcing guidelines that will be implemented in European joint supervision.[25] This tightening of the guidelines essentially means ensuring institutions do not become "empty shells", and that executive responsibility can never be delegated to other parties. The guidelines also describe due diligence process in outsourcing. This should help ensure that institutions are able to oversee and manage all risks, and assess on an ongoing basis the quality and results of the outsourced activities. The EBA also issued new guidance for the use of cloud service providers in 2018.[26] DNB will conduct supervision based on these guidelines.

Even if activities by third parties do not clearly fall under outsourcing, banks must have an adequate risk framework. Banks remain responsible for sound business operations. It is therefore important that they effectively manage their third party risks, by conducting proper due diligence and by having ongoing insight into the risks to which they are exposed to through collaboration with third parties. Banks need to have proportionate control measures put in place, even if the bank considers the activities to not fall under outsourcing.[27]

DNB expects banks to adequately address the risks of innovative technologies in their operational control framework. A concrete example is the use of artificial intelligence applications, such as machine learning. The use of these models – mainly through third parties – must not result in responsibilities being shifted from people to machines. DNB therefore expects banks to clearly specify who bears responsibility for decisions resulting from the use of AI applications. Also decisions based on AI should, just like all other decisions, be sufficiently

25 See Section 3:18 of the *Wft*. The European directives on outsourcing date back to 2006 and are currently being revised by the European Bank Authority (EBA). These guidelines set further requirements for banks' management and governance framework regarding outsourcing, and should result in a more harmonised framework at European level.
26 EBA (2017), "Recommendations on outsourcing to cloud computing service providers". These recommendations were introduced on 1 July 2018.
27 In supervisory practice, there are examples of debates between institutions and supervisors concerning the issue of whether there is formal outsourcing or procurement of a standard service. The EBA's draft guidelines on outsourcing provide a clear definition of outsourcing by specifying "critical and important processes" conducted by third parties. Despite this further clarification, differences in interpretation cannot be ruled out in the future. DNB therefore points out the generic importance of risk control when working with third parties.

traceable and explainable.[28] Finally, organisations must be aware of ethical issues surrounding AI applications, such as the risk of biases through for example the use of distorted information. Because AI applications can add value to banking business while at the same time raising new questions, DNB will conduct further research into this specific theme in the coming period.

In supervision there is growing attention for the operational resilience of institutions. This means that DNB will see to it that banks have plans to ensure they can quickly recommence operations in the event of a failure or disruption at a third party. We expect for example that banks can switch service providers to prioritise continuity of services. The operational resilience requirement currently forms the basis for supervision of core payment infrastructures, but its scope extends to other banking activities.[29]

Banks should focus on the long-term sustainability of their business models. A relevant development is the potential platformification of the sector, and the associated questions of whether banks themselves want to and are able to maintain the primary customer relationships. It is ultimately up to the banks to make this strategic choice. In this respect, it is not only strategic ambition that is relevant, but also the organisation's capacity to change to actually realise this ambition. If banks pursue the role of platform providers, then this implies a far-reaching restructuring of the business model. Capacity development in the area of, for example, data analysis and the selection of third parties fits this role. For banks in the supplier role, the platform is primarily a distribution channel, with fewer possibilities for cross-selling. In this role it is all the more important to maintain a manageable cost-to-income ratio and to keep the cost base as flexible as possible.

5.2 Next steps for supervision

It is important that supervisors gain better oversight and insight into possible concentration risks in outsourcing. This is necessary to be able to place additional requirements on banks in time, should the continuity of services come under threat by single point of failure. As of this year, banks must therefore report material cloud outsourcing,[30] and as of mid-2019 they must also report other material outsourcing arrangements.[31] DNB will systematically identify whether there is a build-up of concentration risks. This also requires looking at subcontracting.[32] If necessary, insights into concentrations will be shared with banks.

The potential concentration risks of for example cloud service providers give grounds for a study as to whether certain service providers must be seen as too big to fail. This issue cannot be addressed nationally, but requires an internationally-coordinated approach. Firstly, because this concerns cross-border services and potential concentrations could pose a global risk. Secondly, because it is essential to gather data at an international level. In due course, it may be considered – at international level – to place the largest service providers, measured by degree of concentration, under a form of supervision. The supervision of third parties in the United States

28 Further specification of traceability and explainability will be the subject of a follow-up study, which will also seek alignment with for example the FSB and the SSM. In terms of traceability, the emphasis is on which steps have been taken in the process for reaching a decision. In terms of explainability, the emphasis is on how the decision has been reached.
29 The Operational Resilience Working Group of the Basel Committee for Banking Supervision (BCBS) plans to carry out a study in 2019 on the desirability of basic principles for operational resilience.
30 EBA (2017), "Recommendations on outsourcing to cloud computing service providers".
31 EBA (2018), "Consultation paper on draft guidelines on outsourcing arrangements".
32 Parties to which critical services are outsourced must notify the bank when they in turn subcontract activities to third parties. If this activity is sufficiently material, then the supervisor should also be notified.

5.1 Focal points for the sector
5.2 Next steps for supervision

(as described in the box on page 16) provides interesting points of reference in this context and may also be desirable at European or international level.[33]

DNB will perform an in-depth policy research into banking revenue models and data utilization by banks. The research into revenue models will focus on the medium term of three to five years. The objective is to both contribute to the public debate on the role of banks, and also to support European supervision of banking revenue models.

An open banking sector calls for broader (statutory) possibilities for cooperation between supervisors with different mandates. In an open banking sector, certain areas such as IT and the use of data by banks and third parties, require coordination between the various financial and non-financial supervisory authorities.

The above-mentioned areas of IT and data fall under the remit of at least five supervisory authorities: the Dutch Radiocommunications Agency is responsible for ensuring compliance with the Directive on security of network and information systems; the Dutch Data Protection Authority ensures personal data is properly processed; the Dutch Authority for the Financial Markets ensures duty of care requirements are met; the Authority for Consumers & Markets sees to it that third-party gain access to the financial sector, and DNB monitors the financial solidity and integrity of institutions. As the interplay between these authorities' remits increases, it is important to ensure proper delineation of each other's responsibilities. In addition, the effectiveness of supervision can be increased by facilitating the exchange of knowledge between different supervisory authorities.

Where necessary and desirable, we will consider, in consultation with our fellow supervisors, whether an extension of existing or additional legal provisions and cooperation agreements is necessary.

33 Concentration risks can also be mitigated through other ways than financial supervision. For example, the European Commission is encouraging cloud service providers to develop codes of conduct and agreements to allow consumers to switch between providers more easily.

This study is partly based on interviews with banks, fintechs, academics and fellow supervisors. We thank all participants for their involvement and insights. Ria Roerink, Danijela Piljic and Kasper Goosen.

5.1 Focal points for the sector

5.2 Next steps for supervision