

PRINCIPLES OF
BANKING
REGULATION

.....

KERN ALEXANDER

obtaining credit from traditional banks because of stricter regulation and previous lack of access to credit.

- 12.7 The disadvantages of P2P lending platforms are several, including the creditworthiness and other information about the borrower and lender are more difficult to ascertain. This leads to a higher risk of default, as the lender cannot rely on the veracity of the information provided on the e-lender's platform and it is difficult for the lender to seek compensation for any defaults. These greater risks are not absorbed by the e-lending platform business and instead are covered by individual lenders – many of whom may be unsophisticated in how they assess credit and other market risks. However, the greater risk of default in P2P lending does not appear to pose systemic risks to the banking sector, as the amount of credit provided through e-lending and other P2P platforms is very limited in comparison to the amount of credit provided by the banking sector as a whole.
- 12.8 However, the number of borrowers is growing rapidly along with limited competition and there is an incentive for some platforms to become too big too quickly. E-lending businesses may not be as sophisticated in managing risks as traditional banks and therefore regulation may have a role to play.

II OPEN BANKING

All banks do is really data, so when you open that data up to third parties it allows for the first time a separation between the person that manages the customer relationship and the person that provides the balance sheet services.¹

- 12.9 The digitisation of banking – particularly in payment services – and the use of access and network technologies has created various opportunities for big data management companies, Fintech firms and challenger banks to increase their respective market share. The European Union adopted Payment Services Directive 2 (PSD2) in January 2016; this introduces a new legal framework to govern the phenomenon of open banking which may transform the provision of banking services. The PSD2 contains an 'access to account rule' which requires all banks and certain other financial intermediaries to provide authorised third-party account providers with access to the bank's customer account records if their customers expressly consent to such third-party access. PSD2 sets out information requirements, rights and obligations of payment service users and providers (PSPs) that facilitate the transfer of funds.

¹ Antony Jenkins, former Barclays chief executive. See Arnold M, Binham C and Brunson J, 'European Banks Brace for Shake-up in Customer Data Access', *Financial Times* (London, 12 January 2018).

- 12.10 The main objective of PSD2 is to increase competition in the provision of banking services. European policymakers adopted PSD2 because they had concluded that banks had operated with very little competition in their markets for too long.² PSD2 requires banks to grant third-party access to their customers' accounts and payment services securely after obtaining customer consent. Prior to PSD2, banks were not required to share customer data with third parties. The third parties who will be granted access to customer accounts under PSD2 are known as *account information service providers* (AISPs). Also, with customer consent, the bank would be required to permit other third parties to initiate payments from a customer's bank account on the customer's behalf to other parties' (i.e. merchants) bank accounts. Under PSD2, these third parties are known as *payment initiation service providers* (PISPs). To access both customers' account information and to initiate payments, a third party must be certified by the financial regulator as an authorised third-party provider (TPP).
- 12.11 The PSD2 provides the legal basis for the unbundling of banking services in a similar way to how telecom services and some utility services were unbundled in many countries in the 1990s and 2000s. The unbundling of banking services is expected to introduce more competition and efficiencies into the banking sector, especially for retail banking customers. The legislation will require banks to notify their customers that they can consent to have their account records and transaction history transferred to third-party service providers who will then be able to review their records and offer them account services, such as lower charges for credit card or foreign exchange transactions. These AISPs can be other banks, financial data management firms and other non-traditional financial service firms as well as retailers, social media and telecom companies. After reviewing bank customer data, they will be allowed to offer them account information services through an online service that will provide aggregated information on one or more payment accounts held by the customer (e.g. balances and payment history) with other payment service providers.
- 12.12 AISPs will also be eligible to obtain a licence by the regulator to become a payment initiation service provider (PSP). PSPs can initiate online payment orders at the request of the customer with respect to a payment account held at another PSP. PSPs can be merchants or third-party payment service providers (e.g. PayPal) which, with the consent of the bank's customer, would be allowed to make payments from the customer's account. AISPs and PSPs are expected to transform the provision of banking services by allowing customers to choose to allow them to advise and offer financial services to them, taking away much of this profitable business from the banks. Some bankers predict that AIP technology, along with the legal framework that facilitates the rise of AISPs and PSPs, will result in an unbundling of banking services similar to the unbundling of the telecoms industry. AISPs and PSPs will be in a position to potentially skim off from the banks the

² *Ibid.*, citing Olle Ludvigsson, Member of the European Parliament stating that PSD2 was needed because '[f]or too long banks have existed in an environment without competition'.

marketing, sale and provision of most banking services, leaving banks merely as infrastructure providers that maintain the balance sheets of their customers.

- 12.13 Although the legislation does not prescribe a particular technology or software program for AISPs and PISPs to access bank customer accounts, the industry standard is known as Application Programming Interfaces (APIs). APIs have been deemed the most reliable and tested technology to facilitate secure and reliable access to customers' accounts, even though the technology is not directly mentioned in the EU legislation.
- 12.14 The PSD2 requires banks to open access to their customers' accounts with customer consent for a wide array of services. For example, the legislation covers the enabling of cash deposits and withdrawals; execution of credit transfers, standing orders and direct debits; payments through cards and similar devices; issuing of payment instruments (such as cards or wallets), money remittances; payment initiation services; and account information services.
- 12.15 The PSD2 open banking legislation would apply in the following hypothetical situation. A customer has a savings account with bank A and another financial product (i.e. a mortgage) with bank B. Prior to PSD2, both banks would have a direct relationship with the customer about their respective products. However, PSD2 provides that either or both banks could lose (with customer consent) the customer, as that relationship would be managed by an AISP. Although the customer would still keep their accounts with both banks and the banks would provide the balance sheet maintenance, the customer's primary relationship would be with the AISP or TPP. Essentially, the AISP or TPP would deal with the bank on the customer's behalf (see Figure 12.1).

A Customer Bank Relationship Today

- 12.16 The PSD2 provides the basic principles for the regulatory framework that would govern the functions and responsibilities of account information service providers (AISPs) and payment initiation service providers (PISPs). Each EU Member State will have a designated regulator that will grant licences to third-party AISPs and PISPs and will ensure that they comply with the relevant data protection laws and financial regulatory framework, particularly to protect against operational risks and related cyber and financial crime risks. The European Supervisory Authorities (the EBA, ESMA and EIOPA) will design technical standards for a risk-based supervisory regime that Member State supervisors can implement and apply across EU states (see Figure 12.2).

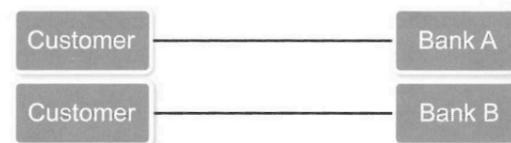


Figure 12.1 Pre-PSD2/open banking

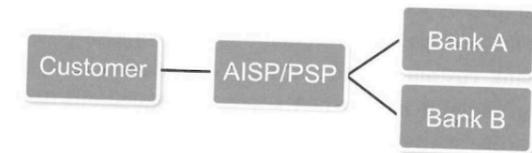


Figure 12.2 Post-PSD2/open banking

- 12.17 The PSD2, along with other similar legislative and regulatory initiatives in other countries (e.g. UK open banking), could well usher in further disintermediation of retail banking services as third parties take over the relationships that banks currently have with their customers. Established banks might have to reconsider their market position and review their strategy for providing value to their customers. This is expected to increase innovation in the sector and thus provide higher transparency, security, quality of service and lower prices for users, especially for retail customers. In addition, it will promote the further integration of the Eurozone and EU payments system, and support a more efficient EU payments market as well as promote competition.

B UK Open Banking

- 12.18 The UK Competition and Markets Authority (CMA) issued the Retail Banking Market Investigation Order 2017. This secondary legislation is similar to, but different in key respects from, the EU PSD2. Article 14 of the Order required the nine largest UK-based banks to make available for release personal current account (PCA) and business current account (BCA) datasets to authorised third-party firms by 13 January 2018 as part of the UK open banking policy.
- 12.19 In late 2017, six of the nine banks informed the CMA that they would not be able to release all the datasets by the specified date. The CMA responded by issuing each of these banks with directions stipulating the timeline for the delivery of the outstanding datasets and the arrangements that each bank must make for reporting progress to the CMA in the meantime. Three of the six banks have complied with the CMA directions as of July 2018, but three have not provided datasets. Although the CMA is responsible for ensuring that covered banks are disclosing the required datasets to authorised third-party firms, the UK financial regulator – the Financial Conduct Authority – is responsible for authorising third-party account service providers and payment service initiators.
- 12.20 In addition, unlike the PSD2, the UK legislation creates a framework that delegates to the regulator (the FCA) the design of an API standard for digital banking. In designing an API standard, the UK Competition and Markets Authority proposed an implementation entity consisting of the nine largest UK banks to make recommendations for the type of agreed

technical standards that would govern the banks' interaction with third-party account providers and the type of API standard to be used for communication and transfer of data between bank customers and third-party service and payment providers. Based on the proposals of the nine banks, the UK adopted regulations that became effective in January 2018 for the use of an API standard and to require that the nine largest UK banks make their customers available to certified third parties.

- 12.21 The UK regulations make it easier for bank customers to compare details of current accounts and banking services across different banking institutions. Over time, though, it is envisioned that the third-party providers, as well as banks, may develop new online and mobile applications, allowing customers to share data securely across different regulated institutions – both financial firms and data service providers. The Competition and Markets Authority and the Financial Conduct Authority have adopted regulations to certify third-party account service and payment providers that are similar to AISPs and PSPs under the PSD2, but significant differences exist between the two regimes.
- 12.22 Regarding the API standard, the PSD2 does not require the creation of a common API standard. This allows individual banks to make their data available through different technical standards, which may create additional complexity for the use of account aggregation tools. In contrast, the UK open banking regulation requires the creation of a common API standard across banks and third-party providers.
- 12.23 For customer data transfer, the PSD2 permits customer account data to take place through a method known as 'screen scrapping', in which customers who agree to provide their account details are required to provide their login details to third-party companies who can subsequently login and obtain their financial information. However, the UK regulations do not require customers who have agreed to provide their account details to provide login details to the third-party providers. Rather, customer data is transferred to the TPP by using a 'plug' and 'socket' approach, in which third-party firms can connect directly to the banks in order to access the data that the customers have consented to provide.

C Covered Institutions and Disintermediation

- 12.24 The definition of covered institutions that are required to be certified in order to provide third-party account and payment services varies between the UK regulation and the EU PSD2. Under PSD2, third-party providers must be either a certified account information services provider (AISP), a payment initiation provider (PIP), or both (TPP). The UK regulations, however, permit a broader range of third parties to provide these services. They would be authorised through a process called 'white-listing'. For example, price comparison websites that customers might use to compare the prices and services of different banking products do not fall with the coverage of PSD2 and therefore would not be regulated as an

AISP. But the UK open banking regulations would ensure that these web-based information providers were certified and regulated under the regulation's 'white-listing process'.

- 12.25 The long-term trend caused by the open banking phenomenon is the potential disintermediation of banks from the provision of many retail and some wholesale banking services. Banking industry studies estimate that banks face more disintermediation risk than payment service providers, because payment firms have already adapted to data provision markets.³ Banks may be forced to compete not merely against other banks but also against many other financial firms and third-party account service providers for account management and products. Also, the increased competition created by PSD2's liberalisation framework for bank account service provision may result in reduced bank profit margins and lead to increased volatility in the value and number of deposit accounts. It could also decrease the volume and sources of bank funding and, in turn, their lending capabilities.
- 12.26 The short-term trends in open banking are the following: increased regulation driven in part by PSD2 principles-based regulatory standards that are proposed and adopted by the European Supervisory Authorities and later implemented by Member State authorities. The wave of regulation may come before the market converges on any one API standard or particular business practice of third-party account providers. Also, an important question is to what extent will bank customers consent to have their data accessed by these third-party providers? The technical obstacles of implementing the necessary technology infrastructure and account interface protocols for third-party providers with banks and their customers is not yet fully known.

III DIGITAL CURRENCIES AND BITCOIN

- 12.27 Bitcoin was created in 2009 by an anonymous person named Satoshi Nakamoto, who developed a block-chain technology that allows individuals who access the technology to trade Bitcoin between themselves without the involvement of banks or other intermediaries such as central banks. Bitcoin is an example of a digital or virtual currency – other digital currencies include Ethereum, XRP, Stellar, Cardano – which many users believe will eventually replace central bank currencies ('fiat money') and banks themselves with new virtual currencies that can be traded directly between individuals without the involvement of banks or other intermediaries. The value of Bitcoin, like gold, depends on demand and supply, with the supply limited because Bitcoins must be 'mined' in a complex, virtual system. The growing popularity of Bitcoin, and other virtual currencies, has led to significant increases in its price and to a growing number of individuals buying and selling Bitcoin on unregulated exchanges, often leading to volatile price movements that are

³ See Ghose R, *Bank of the Future: The ABCs of Digital Disruption in Finance* (Citi GPS: Global Perspectives & Solutions, March 2018), 60.