

Digitalisation of payment services

Fernando Zunzunegui¹

Profesor de Derecho del Mercado Financiero, Universidad Carlos III de Madrid

fernando.zunzunegui@uc3m.es

ABSTRACT

This paper studies the advantages and challenges of digital payments. Large banks are transformed into platforms that share clients without losing control of the business. We are facing an open banking that combines finance and technology offering safety in a digital environment. These changes involve important regulatory challenges. The model of the European Union becomes a universal reference. It forces Banks to share customer data with technology firms. It prioritizes giving clients the power over their data with the security offered by the access through APIs. It gets right by combining financial regulation with data protection. It encourages innovation in a regulated framework. The objective is to reconcile innovation with the safety and stability of the financial system.

Keywords: Open Banking, PSD2, API, Digital Payments, Fintech, Data Protection, Financial Regulation, Client Protection

¹ This paper was originally published in the Working Paper Series of the Ibero-American Institute for Law and Finance (available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256281). I would like to thank Professor Aurelio Gurrea and Professor Nydia Remolina for the comments they made during the writing of this chapter within the framework of research project DER 2017.83321-P “Protection of consumers and customers of Fintech services”.

SUMMARY: 1. INTRODUCTION. 2. ADVANTAGES AND CHALLENGES OF DIGITAL PAYMENT SERVICES. 3. FROM THE MONEY BUSINESS TO THE DATA BUSINESS. 4. TOWARDS AN OPEN BANKING MODEL. 5. REGULATORY CHALLENGES. 6. PSD2 AS A UNIVERSAL REFERENCE MODEL. 7. COMMUNICATION GATEWAYS (API). 8. SECURITY IN DIGITAL PAYMENTS. 9. CONCLUSIONS.

1. Introduction

Payment services are the testing ground for Fintech. In fact, in some areas of academia, the term “Fintech” has always been associated with new payment card technologies². Technology applied to payment services is nothing new. ATMs, card systems and e-money, mobile banking and, generally speaking, means of payment and financial services channels, require heavy investment in technology. What has changed is the business model and the actors involved in the value chain. Tech companies, in particular American (GAFA) and Chinese (BAXT) tech giants,³ are competing with the banks. They use customer data to offer new financial services. Technology is used to improve the efficiency of financial services by making them more accessible, faster and cheaper. In the payment system, technology also speeds up payments and lowers their cost, and creates new instruments and services. Cryptocurrencies and payment initiation or information management services associated with bank accounts have emerged.

The purpose of the business is also changing. The banks have always innovated in the provision of payment services but did not go so far as to use customer data as the main purpose of their business. Banks considered the focus of their business to be money and securities and they viewed customer data more as a liability than an asset, something they had to protect. However, tech companies see customer data as the focus of their business. These companies monetise data in two ways. On the one hand, data use is the main source of their income; and on the other hand, they turn data into a bargaining chip. Services that are apparently free, such as search engines, are paid for by assigning data.

² See Marc Hochstein, *BankThink Fintech (the Word, That Is) Evolves*, AMERICAN BANKER, 5 October 2015, available at: <https://www.americanbanker.com/opinion/fintech-the-word-that-is-evolves>; Douglas W. Arner, Janos Nathan Barberis, Ross P. Buckley, *The Evolution of Fintech: A New Post-Crisis Paradigm?*, UNIVERSITY OF HONG KONG FACULTY OF LAW RESEARCH PAPER, 2015/047 (October 1, 2015), available at SSRN: <https://ssrn.com/abstract=2676553>.

³ GAFA (Google, Apple, Facebook and Amazon) and BAXT (Baidu, Alibaba, Xiaomi and Tencent). Regarding the Chinese experience, see Zennon Kapron, *From digital payments to digital finance: How China’s tech companies are redefining banking in Asia and soon Europe*, 12.1, JOURNAL OF PAYMENTS STRATEGY & SYSTEMS, 68 (2018).

The financial economy is giving way to the data economy⁴ in which handling data is essential to economic success⁵. We are living in a time of platform capitalism⁶ in which banks face the risk of losing control of their customers. Just as there are transport platforms without cars, rental platforms without apartments and sales platforms without products, financial services platforms can also be developed without the need to open current accounts, the economic basis of the traditional banking business. Such platforms would have customers with current accounts open in banks that have no special relationship with customers, as they have stopped regularly using their services. It is not envisaged that payment services will be unlinked from bank card accounts in the near future. To take that step it would be necessary for cryptocurrencies to be established as currency, i.e. as a widespread means of payment⁷.

In this context, new payment applications are displacing cash. Cash withdrawals from ATMs are falling. Payments are increasingly digital. Financial authorities and governments are promoting a reduction in cash use on security and efficiency grounds. High-denomination notes are being withdrawn⁸. The traceability of digital payments makes it easier to monitor payment movements.

Until the Fintech industry emerged, customer data were captured by the banks but not exploited to expand the business. There were no data-processing programs. Now Big Data and artificial intelligence makes it possible to extract value from data. On this occasion, innovation has not

⁴ Viktor Mayer-Schönberger, Thomas Range, *REINVENTING CAPITALISM IN THE AGE OF BIG DATA* (Basic Books, Business & Economics, 2018), who state that: “A recent confluence of advances in data-handling is finally enabling us to leave behind the limitations of money and price and embrace data-richness on markets” (p. 64).

⁵ Darcy Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, Jason Potts, *Some Economic Consequences of the GDPR*, 1 (May 23, 2018), who say: “Personal data is an economic good that is valuable and when linked to other data creates further value”, available at: <https://ssrn.com/abstract=3160404>.

⁶ Regarding platforms as a hegemonic model of modern capitalism, see Nick Srnicek, *PLATFORM CAPITALISM* (Polity, 2017). The terminology is not well-established. For an approximation of the taxonomy of financial platforms see Pascal Bouvier, *Platform Banking Taxonomy*, 16 October 2016, available at: <https://finiculture.com/platform-banking-taxonomy/>

⁷ Regarding the systemic risk created by cryptocurrencies, see Nicholas Weaver, *Risks of cryptocurrencies*, 61.6, *COMMUNICATIONS OF THE ACM*, 20 (2018).

⁸ For India and the European Union, see Ravi Kumar Goriparthi, Pankaj Tiwari, *Demonetization in India an Era for Digital Payments*, 4.1, *SPLINT INTERNATIONAL JOURNAL OF PROFESSIONALS*, 40-48 (2017); and the European Central Bank, *ECB ends production and issuance of €500 banknote*, Press Release, 4 May 2016, available at: <https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html>

come from development of the traditional banking business but instead from these data technologies. The banks have closed, rigid systems, built through sedimentation, in contrast to tech companies' open and flexible systems.⁹

Retail banking is the most affected by the appearance of Fintech and, in this context, the payment system is in the vanguard of the financial market's transformation. In payment services, the regulator is driving economic progress forward. It is opening banking customer data up to third parties. This is a structural change that allows the digital business to emerge¹⁰. It contributes to disintermediation of payment services. It removes the barrier to tech companies entering the payment business in their own right. They can choose the service to be provided, cutting costs and regulatory compliance risk.

The banks have reacted in various ways to the emergence of technologies in the financial market and payment services in particular¹¹.

- They can restrict themselves to complying with the new legal framework.
- They can maintain their universal banking model, offering all kinds of financial services by creating and distributing their own products. Fintech companies have emerged as a new sales channel, a modern way of accessing customers. Rebates and other forms of commission are established to pay the Fintech marketing companies.
- They may choose to continue to produce financial products but leave distribution in the hands of third parties. However, they assume the risk of becoming a mere infrastructure.
- Based on the background in the tech sector, the option consulting firms advise is to share data and extend the business,¹² either by transforming themselves into application

⁹ Autorité de Contrôle Prudentiel et de Résolution (ACPR), *Étude sur la révolution numérique dans le secteur bancaire français* (2018), available at: https://acpr.banque-france.fr/sites/default/files/medias/documents/as_88_etude_revolution_numerique_secteur_bancaire_francais.pdf

¹⁰ World Economic Forum, *Beyond Fintech: A Pragmatic Assessment of Disruptive Potential in Financial Services*, part of the Future of Financial Services series, Prepared in collaboration with Deloitte (2017), available at: http://www3.weforum.org/docs/Beyond_Fintech_-_A_Pragmatic_Assessment_of_Disruptive_Potential_in_Financial_Services.pdf

¹¹ See Lael Brainard, *Where Do Banks Fit in the Fintech Stack?*, Northwestern Kellogg Public-Private Interface Conference on New Developments in Consumer Finance: Research & Practice (April 28, 2017).

¹² PWC, *Opening the bank for a new era of growth* (June 2018), which concludes: “Despite some skeptical views on a more open approach, many financial services firms already provide access to internal core systems and share consumer data with third parties. In further embracing this strategy, organizations can potentially accelerate efforts to revitalize growth in banking”, available at

platforms, as in Apple's business model¹³, or by creating a market for the distribution of products and services open to third parties¹⁴.

In fact, banks are reacting to competition from tech companies and transforming themselves into Fintech businesses¹⁵. The business models are converging¹⁶. Tech companies are entering the regulatory compliance culture of the banks and financial institutions are learning to exploit their databases just as tech companies have. It is a more efficient model that cuts costs and increases the quality of service. There is a trend towards integration of the Fintech industry and the traditional financial services industry.

There are those who think that the Fintech sector “*may emerge as a complement to rather than a substitute for the banking business*”¹⁷. The competitive advantage offered by technology is only

<https://www.pwc.com/us/en/financial-services/publications/assets/pwc-fs-digital-open-banking.pdf>;

Deloitte, *Open banking: A seismic shift* (June 2017), according to whom: “*Financial institutions will need to learn to operate in a shared ecosystem, moving away from the currently closed environment to one where they need to work more closely with third parties*”, available at <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-seismic-shift-180118.pdf>

¹³ See Hendrikse Reijer, David Bassens and Michiel van Meeteren, *The Appleization of finance: Charting incumbent finance's embrace of FinTech*, FINANCE AND SOCIETY, 1-22 (2018).

¹⁴ The impact of technology is being magnified by large international consulting firms. Their message is clear: “*the forces of change are inevitable. Banks are better served getting ahead of and defining the trend rather than waging a futile battle to repel it*”, cf. Laura Brodsky, Liz Oakes, *Data sharing and open banking*, MCKINSEY & COMPANY (2017), available at: <https://www.mckinsey.it/sites/default/files/data-sharing-and-open-banking.pdf>. In particular, Fintech's impact on payment services may be overestimated, see Olly Jackson, *PSD2 gives banks chance to evolve*, INTERNATIONAL FINANCIAL LAW REVIEW (January 26, 2018).

¹⁵ In fact, there are tech companies that are entering the financial sector (Tech-Fin) and banks that are taking on technology companies' business models (Fin-Tech). See C. Schena, A. Tanda, C. Arlotta, G. Potenza, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, 1, QUADERNI FINTECH, 100 (2018).

¹⁶ Giorgio Barba Navaretti, Giacomo Calzolari, Alberto Franco Pozzolo, *FinTech and Banks: Friends or Foes?*, EUROPEAN ECONOMY, 2 (2017), according to which “*the future of the financial industry will be shaped by the convergence of surviving incumbent banks and more “organic” FinTech Operators*” (p. 27).

¹⁷ Santiago Carbó, *Mitos y realidades de la digitalización financiera: los medios de pago como paradigma*, MEDITERRÁNEO ECONÓMICO, 29 (March 2017), p. 146, available at <http://www.publicacionescajamar.es/pdf/publicaciones-periodicas/mediterraneo-economico/29/29-773.pdf>

relevant in the short term¹⁸. Banks are acquiring tech companies¹⁹ or reaching agreements with better established ones²⁰.

The banks are facing new competitors enabled to provide the new information and payment initiation services. However, the development of new businesses is being channelled towards cooperation in an environment controlled by the banks under the watchful supervision of central banks and banking supervisors. Even the more open authorities, such as those in the United Kingdom, are cautious about the emergence of technologies in finance.

The development of digital payments depends on cooperation to create standards and platforms for products and services. It also depends on the degree of concentration in the industry. New infrastructures are expensive and require a shared effort. Hence the authorities' drive towards banking concentration. Such concentration encourages the implementation of new technologies but also creates risks. Neobanks are acquiring market power and compromising competition, creating a risk of financial exclusion for people without resources or technological skills. The European Banking Authority (EBA) is thus analysing the financial exclusion that may be caused by the algorithms used in Big Data²¹.

2. Advantages and challenges of digital payment services

Digital payments and, generally speaking, use of new technologies in the financial industry has clear advantages. On the one hand, costs are lowered and it is easier to access the financial sector. Consequently, in addition to reducing the cost of lending, which benefits individuals and companies, it may also contribute to reducing the problems of financial exclusion that exist in

¹⁸ Giorgio Barba Navaretti, Giacomo Calzolari, Alberto Franco Pozzolo, *FinTech and Banks: Friends or Foes?*, EUROPEAN ECONOMY, 2 (2017), p.16.

¹⁹ See the acquisition of WePay by JPMorgan.

²⁰ See Wharton University of Pennsylvania, *Banks and Fintechs: Adversaries or Partners?* (2018), available at: <http://knowledge.wharton.upenn.edu/article/banks-fintechs-adversaries-partners/>

²¹ European Banking Authority, *The EBA's Fintech Roadmap. Conclusions from the consultation on the EBA's approach to financial technology (Fintech)*, 260 (2018), available at: <https://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf>; European supervisory authorities have also warned of this risk, see Joint Committee of the European Supervisory Authorities, *Joint Committee Final Report on Big Data*, 11-14 (2018), available at: https://www.esma.europa.eu/sites/default/files/library/jc-2018-04_joint_committee_final_report_on_big_data.pdf

many countries, especially in emerging economies²². In addition, it improves the "customer experience", which is an essential aspect of the commercial relationship.

Moreover, digitalisation of means of payment makes it possible to create new products and services in a more efficient market. Users want to make secure payments in a straightforward, almost imperceptible manner. They also want them to be immediate and very low cost. They want payment instruments that are easy-to-use, always available and online. Payment is integrated in the commercial operation (all-in-one). There is a trend towards dilution of payments in commercial business²³. However, payment is and continues to be a complex process in which many different operators and clearing and settlement houses participate.

Such ease-of-use puts consumers at risk of rushing into things and overspending. They are universal services provided without restrictions. Payments are accompanied by new tools that consumers can use to check their budget and rationalise their expenditure. Online advances are offered in keeping with the digital profile, which poses a risk of overindebtedness²⁴. Payment platforms make it possible to generate digital profiles that can be used to assess the necessary creditworthiness for loans. The market is becoming segmented, which poses a threat to the universal banking system. The customer stops interacting with the bank to make the payments.

These are advantages and challenges posed by digitalisation of payment services. There is consensus that digitalisation of payments is socially beneficial. The immediacy of payments may have an effect on GDP similar to that which ATMs had in the last century²⁵. The challenges

²² See Paulo L. dos Santos, Ingrid Harvold Kvangraven, *Better than Cash, but Beware the Costs: Electronic Payments Systems and Financial Inclusion in Developing Economies*, 48.2 DEVELOPMENT AND CHANGE, 205-227 (2017). Regarding the importance of digital payments in financial exclusion, India is a very relevant case to watch. See Arunava Ghosh, *Turning India into a cashless economy: The challenges to overcome* (June 21, 2017), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2989290; and Mrunal Chetanbhai Joshi, *Digital Payment System: A Feat Forward of India* (October 11, 2017), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043609

²³ Max Geerling, *E-commerce: A merchant's perspective on innovative solutions in payments*, 12.1, JOURNAL OF PAYMENTS STRATEGY & SYSTEMS, 58-67, (2018), "less visible", "reducing 'the pain' of payment for the consumers" (p. 61).

²⁴ Regarding the risks associated with new services based on digital profiles, see Antonello Soro, *Fintech e Diritto*, ABI - Inaugurazione Corso di alta formazione "Fintech e Diritto", 10 May 2018, Rome, available at: <http://www.antonellosoro.it/2018/05/10/fintech-e-diritto/>

²⁵ Monika Hartmann, Lola Hernández, Mirjam Plooi, Quentin Vandeweyer, *Are Instant Retail Payments Becoming the New Normal? A Comparative Study*, EUROPEAN CENTRAL BANK, 3 (2017).

notably include lack of digital knowledge among users, the risk Fintech companies face with the burden of regulatory compliance, and the legal risk of central banks providing current accounts for the public.

In this area of the payment system, consumers must authorise the use of their data and control how they are used. However, they lack sufficient digital knowledge. They are unaware of the risk of giving the "key to their data" to third parties other than the bank in which they have placed their trust so that third parties can initiate payments or manage their account information. The data may be used to exploit consumers' biases or simply to allow greater price discrimination between consumers.

Tech companies that are entering finance are positioned as sales intermediaries between the bank and the customer. This weakening of the customer relationship affects the traditional banking business. Digitalisation is associated with outsourcing that poses risks. The banks come to depend on tech service providers. As a consequence of the so-called Tech-Fin²⁶, banks face fierce competition in unfamiliar territory, the data market. They face the legal risk of data misuse. They are well-versed in regulatory compliance within the financial system but they are new to the data industry. The same caution tech companies feel about entering the financial business—an overregulated sector with a very high burden of regulatory compliance—is felt by banks when they enter the data market, which has few clear rules and a great risk of heavy fines²⁷.

However, the main threat to deposit banking that provides current accounts does not come from tech companies. The threat comes from proposals aimed at allowing central banks to open current accounts for the public²⁸. There is a trend towards eliminating cash and completely replacing it

²⁶ Jack Ma, CEO and founder of Alibaba, was the first to use the term *TechFin*, which refers to non-financial companies, such as telecom, tech and e-commerce companies entering the financial services business. See Dirk A. Zetsche, Ross P. Buckley, Douglas W. Arner, Janos Nathan Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 6, EBI WORKING PAPER (2017), available at

<https://hub.hku.hk/bitstream/10722/241271/1/Content.pdf?accept=1>

²⁷ Fines can be as much as €20 million or 4% of turnover, whichever is higher (art. 83.6 GDPR).

²⁸ Aleksander Berentsen, Fabian Schar, *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*, 100.2, FEDERAL RESERVE BANK OF ST. LOUIS REVIEW, 97-106 (2018), available at <https://doi.org/10.20955/r.2018.97-106>. Ideas gathered in Spain by Miguel Ángel Fernández Ordoñez, *Un dinero revolucionario*, EL PAÍS (20 April 2018), available at:

https://elpais.com/elpais/2018/04/11/opinion/1523444783_459700.html

with digital money²⁹. There is a move towards stripping banks of the power to create money³⁰. This is a return to the 19th century, when central banks opened current accounts for savers.

Digital money is currently banking money that operates in a centralised manner with the help of clearing houses. Fintech has fostered the creation of cryptocurrencies such as Bitcoin, which operate in a decentralised and distributed manner. In response to these private systems, it has been proposed that public digital currencies should be created. This aim would be achieved by allowing central banks to open current accounts for the public. This would meet the need for a secure currency without the risk of freezing bank account withdrawals. Accounts open in the central bank would be a refuge during financial crises. In view of the distrust of private currencies, funds would be transferred into the account open in the central bank. Private banks could continue to provide services to the holders of central bank accounts but they would do so as payment initiators or managers of account information. Their business model would be transformed. Instead of providing accounts, they would be third-party providers of services to the central bank, which would provide the accounts. This proposal should be viewed negatively. The response to traditional banks' problem with their reputation, which was damaged by the financial crisis, and the emergence of Fintech services, should be found in the market.

3. From the money business to the data business

Bank users' trust fell when the financial crisis began in 2008³¹. However, banks are still trusted by customers as custodians of funds. Now, in order to compete with Fintech companies, they need to gain their trust as custodians of their data.

Banks see their customers' data as a custodial responsibility rather than a business opportunity. They are now discovering that they have a mine of data that they can use to expand their business. The dataflow has multiplied by 80 in a decade³² and the cost of managing the data is ten times

²⁹ Kenneth S. Rogoff, *THE CURSE OF CASH* (Princeton University Press, 2016).

³⁰ See International Movement for Monetary Reform (<https://internationalmoneyreform.org>).

³¹ See *2010 Edelman Trust Barometer* (January 22, 2010), according to which: “*Since 2007, trust in banks declines dramatically in most Western countries. In U.S., trust in banks drops from third to near-last in three years*” (p. 15), available at https://cms.edelman.com/sites/default/files/2017-03/2010-Edelman-Trust-Barometer_Global_Deck_FINAL.pdf.

³² The flow multiplied by 80 between 2005 and 2016, see Susan Lund, James Manyika, *Defending digital globalization*, MCKINSEY & COMPANY (April 20, 2017), available at: <https://www.mckinsey.com/mgi/overview/in-the-news/defending-digital-globalization>

lower, which has exponentially increased processing possibilities³³. Electronic communications' marginal cost of close to zero is promoting the development of the data market³⁴. The banks never imagined that they would be able to convert their customer data into an essential part of their business. They can offer their data to tech companies to create new products and provide new services. They are thus creating a market in the interests of their customers and for their own benefit.

These innovations are transforming banks into platforms for the distribution of financial products and services. They share objectives with the new entrants. In order to develop these new businesses, they must create secure infrastructure so that tech companies can work with their customers' data. This collaboration allows them to cut the cost of integrating systems, which hitherto accounted for the largest part of the cost of technological changes in the payment system.

The most likely outcome is that the banks will be strengthened by expanding their business through external providers that offer their services on the new platforms³⁵. It is basically large banks who have the means and vision to take advantage of the opportunity³⁶. However, there are those that argue that proximity banking—i.e. serving local businesses and households—may also benefit from the use of new applications³⁷. They are easy to implement. Using them is a cultural problem rather than a resource problem.

³³ See McKinsey Global Institute, *Digital globalization: the new era of global flows* (2016), available at: <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx>.

³⁴ See Jeremy Rifkin, *The Zero Marginal Cost Society* (St. Martin's Griffin, 2015), which mentions that: "Researchers are just beginning to experiment with a new way of storing data that could eventually drop the marginal cost to near zero" (p. 86).

³⁵ Olly Jackson, *PSD2 gives banks chance to evolve*, INTERNATIONAL FINANCIAL LAW REVIEW (January 26, 2018).

³⁶ There may be restrictions on competition. "The risk lies in the exploitation of their position by incumbents, be it large financial institutions or big technology companies, to deny newcomers access to the market" is the opinion of A. F. Carmona, A. G. Q. Lombardo, R. Rivera, C. Pastor, J. V. García, D. R. Muñoz, L. C. Martín, *Competition issues in the Area of Financial Technology (FinTech)* (July 2018), p. 85, available at: [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU\(2018\)619027_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU(2018)619027_EN.pdf)

³⁷ See Camden Fine, *Digitalisation financiera: el community banking en la era de la disrupción digital*, 149 *PAPELES DE ECONOMÍA ESPAÑOLA*, 2-20 (2016).

The difficulties of regulatory compliance and obtaining a banking licence limit the entry of tech companies into the financial business. In the short and medium term, the banking business will remain in the hands of the banks. Most customers prefer not to share their banking data with third parties unless they clearly know what they are going to receive in exchange and what risks they face³⁸.

It is the model for conducting the banking business that will change. We are moving towards a confluence between banks that are becoming tech companies capable of exploiting their customers' data through Big Data, artificial intelligence, Machine Learning and Deep Learning (Fin-Tech), and tech companies that dominate this data traffic that are entering the finance business (Tech-Fin).³⁹ After this transition, a new banking model will arise based on data technology from banks that operate as platforms. New "data banks" that operate with money and data. Just as e-mail coexisted with the postal service until it replaced it, digital banking will be transformed into the new data banking in a few years, regardless of whether it is conducted by the traditional banks or tech companies.

In the European Union, Directive 2015/2366 on payment services (PSD2) gives customers power over their data just as they already had over the funds in their account. Under this directive, customers can authorise third-party providers to access their data and the bank cannot refuse to assign the data, apart from specific exceptions.

There is a parallel between the financial market and the data market. Both of them are based on trust. They are grounded in fiduciary relationships. Without trust users will stop providing the raw material, whether cash or data. They are dematerialised markets. Cash is now somewhat marginalised. Currency is recorded just like data. They are digital records. Moving the balance or

³⁸ According to a report by Accenture, in the United Kingdom, two thirds of consumers are not willing to share their banking data with third-party service providers. See Emma Dunkley, *UK banks prepare to share customer data in radical shake-up*, FINANCIAL TIMES (November 27, 2017). Similarly, "two-thirds (66%) of people would be concerned about how their personal financial data might be used", Ipsos MORI, *Open Banking – are consumers ready?* (November 1, 2017), available at <https://www.ipsos.com/ipsos-mori/en-uk/open-banking-are-consumers-ready>. However, around 80% of digital customers accept data sharing, although a third do so in exchange for faster and easier-to-use services, see Accenture, *Building the future-ready bank. Banking Technology Vision 2018* (2018), p. 16, available at: https://www.accenture.com/t20180418T194011Z_w_us-en_acnmedia/PDF-75/Accenture-Banking-Technology-Vision-2018.pdf.

³⁹ See Dirk A. Zetsche, Ross P. Buckley, Douglas W. Arner, Janos Nathan Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 6, EBI WORKING PAPER (2017), available at <https://hub.hku.hk/bitstream/10722/241271/1/Content.pdf?accept=1>

data requires an order by the customer. The account holder's express consent is required to transfer cash or assign data. The difference lies in their value. Account balances have a monetary value. They are banking money. Data do not have the liquidity of an account balance. However, monetisation of data makes the value of data more similar to that of an account balance. In fact, data are already being used to pay for digital purchases. The Proposal for a Directive on certain aspects concerning contracts for the supply of digital content covers digital content provided not only in exchange for a cash payment but also in exchange for data⁴⁰. Account balances can only be moved between authorised organisations. However, data may be assigned to any person with the technical resources to handle them. Nevertheless, bank account data can only be assigned to authorised organisations. At least that is the principle established in the European Union, in PSD2, which is inspiring the regulations of other jurisdictions.

4. Towards an open banking model

Open banking combines banking and technology, offering the security of banks within a digital environment. There are various definitions of open banking.⁴¹ All of the definitions allude to a new banking model that is open to external providers. Banking is opening up to sharing customers without losing control of the business.

There is a trend towards open banking in line with the model of tech companies with platforms or application markets. There is a movement away from a reserved model in which only banks can provide banking services to an open model in which the banks compete with all kinds of companies, including tech companies. The banks are being transformed into platforms, infrastructures that provide their customers with access to the most diverse financial services. These platforms facilitate ongoing communication with customers and strengthen the fiduciary relationship on which the financial business is based.

⁴⁰ European Commission, *Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, Brussels, 9.12.2015, COM(2015) 634 final, 2015/0287 (COD), which states: “*The vast majority of consumers, Member States and legal professions are in favour of covering digital content supplied not only for a price but also in exchange for (personal and other) data provided by consumers*” (p. 8).

⁴¹ “Open banking is the provision of services in the context of users through API platforms, app stores and apps”, according to Gartner, *Hype Cycle for Open Banking* (July 23, 2013), available at: <https://www.gartner.com/doc/2556416/hype-cycle-open-banking->

Open banking allows customers to control their data and access new, more efficient third-party services under better conditions. It is a new paradigm⁴². It changes the structure of retail banking⁴³. The payment system is where this transformation can be most clearly seen.

The first country to offer a government programme for the transition towards open banking is the United Kingdom. It was promoted by the competition authority in that jurisdiction⁴⁴. The Australian government has made an open banking proposal based on the Farrell Report⁴⁵. The United States is moving more slowly⁴⁶. The diversity of financial authorities stands in the way of federal solutions that adopt the open banking standards of the European Union. Progress towards standardisation of communication channels between the banks and Fintech companies is coming from the private sector⁴⁷. The initiative of the Office of the Comptroller of the Currency (OCC) to create a Fintech banking statute is immersed in intense debate⁴⁸.

⁴² Diana Milanese, *A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States*, 29, TTLF WORKING PAPERS (2017), *passim*.

⁴³ Nick Caley, *What PSD2 and open banking means for financial services in 2018* (March 7, 2018), available at: <https://www.worldfinance.com/banking/what-psd2-and-open-banking-means-for-financial-services-in-2018>, as a catalyst for digital innovation.

⁴⁴ Competition and Markets Authority, *CMA paves the way for Open Banking revolution* (August 9, 2016), available at: <https://www.gov.uk/government/news/cma-paves-the-way-for-open-banking-revolution>

⁴⁵ Australian Government, *Review into Open Banking: giving customers choice, convenience and confidence* (2017), available at: <https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-For-web-1.pdf>. This proposal has the backing of the Australian Banking Association, though with some nuances, as they want to have their own API standards as opposed to the United Kingdom standards adopted in the report, and maintain control of security. See Australian Banking Association, *Response to the Farrell Report into Open Banking* (March 23, 2018), available at: <https://static.treasury.gov.au/uploads/sites/1/2018/04/T282002-Australian-Banking-Association.pdf>

⁴⁶ See Bryan Yurcan, *Open banking's early adopters bet on 'tremendous gains in value'*, AMERICAN BANKER (February 1, 2018), available at: <https://www.americanbanker.com/news/open-bankings-early-adopters-bet-on-tremendous-gains-in-value>. First they want to educate customers and avoid errors that may damage their trust in the banks. Regarding this, see Paul Schaus, *How U.S. can avoid U.K.'s mistakes in open banking*, AMERICAN BANKER (February 2, 2018), available at: <https://www.americanbanker.com/opinion/how-us-can-avoid-uks-mistakes-in-open-banking>

⁴⁷ See Hakan Eroglu, *The American way of Open Banking regulation* (August 16, 2018), available at: <https://www.finextra.com/blogposting/15665/the-american-way-of-open-banking-regulation>, which concludes that: “In the US, open banking is not required by regulators; however, the need to compete with innovations coming from fintechs and other banks may force them to adopt open banking through secure APIs.”

⁴⁸ See Office of the Comptroller of the Currency, *OCC Begins Accepting National Bank Charter Applications from Financial Technology* (July 31, 2018), available at: <https://www.occ.gov/news->

The European Union allows banks' customers to access their data just as they can access the money in their accounts. If the customer consents, the banks must make their bank data available to tech companies. Customers can thus make use of the value provided by data and access new services in exchange for their data. The model developed by tech companies of accessing data in exchange for providing services is used.

In order to better understand the notion of open banking, one should distinguish between banking services that are essential and those that are not. The essential function of the banks is capturing deposits and providing current account credit. This function is not shared in the open banking system. Third-party providers, tech companies, can access bank data—with the customer's express authorisation—and offer all kinds of services. It is prohibited for them to open and manage accounts in the manner of banks. They have to apply for a banking licence to do that. In other words, they have to become banks. This reservation of the banks' essential business is necessary in order to maintain stability and public trust in the banking system.

Other accessory services such as payment initiation and managing the information in payment accounts can be outsourced to trusted third parties who are authorised to provide these kinds of services. The data strictly necessary to provide the service are shared. Sensitive data that are not essential to provide the service must not be shared. Data are considered sensitive when they can be used to commit fraud. They include personal security credentials, i.e. the security details that the supplier provides to the user for authentication purposes in order to verify the user's identity⁴⁹.

Open banking allows greater protection of the most vulnerable customers. Access to the set of banking data makes it possible to warn of overindebtedness and predict loan defaults. It can contribute to improving the customer's financial health.

[issuances/news-releases/2018/nr-occ-2018-74.html](https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf). Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies* (December 2016), available at: <https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf>; Nathan Brownback, V. Gerard Comizio, Fried Frank, *State Bank Regulators Challenge OCC's Authority to Issue Fintech Charters* (June 4, 2017), available at: <https://corpgov.law.harvard.edu/2017/06/04/state-bank-regulators-challenge-occs-authority-to-issue-fintech-charters/>

⁴⁹ See European Banking Authority, *Final Report Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, EBA/RTS/2017/02, 125 (2017), available at:

[https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+\(EBA-RTS-2017-02\).pdf](https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+(EBA-RTS-2017-02).pdf)

In this area, open banking poses a risk of infringements for which the banks assigning the data may be held responsible. Since data are the main asset of digital banking, they are also a source of liability. When data are transferred between banks and new providers, there is a risk of unlawful use and access to customer data. The responsibilities of the banks and the new providers must be defined taking into account that the relevant aspects are protection of the customer and the stability of the financial system.

5. Regulatory challenges

The digitalisation of means of payment and, generally speaking, use of new technologies in the financial sector also presents many challenges to the financial regulators. It is a system of increasing complexity⁵⁰, which involves a paradigm shift in financial regulation⁵¹. The digitalisation of means of payment must thus be part of the financial regulators' action plan⁵² but from a perspective of technological neutrality.

Regulating digital payments is a tough task⁵³. Supervisors are monitoring digital payment services and their impact on the current payment system in order to redefine the perimeter of regulated financial institutions. Cyber security, data protection, the systemic risk of payment platforms and user protection are being analysed. Best practices are identified in order to maintain strong consumer protection. There is room for self-regulation of financial technology.

In general, the Fintech industry has developed in an unregulated environment quite different to financial regulations and their compliance requirements. There is regulatory arbitration that casts doubt on whether there is a level playing field. The authorities were ignorant of the technical side

⁵⁰ These aspects are analysed by Dan Awrey, *Complexity, Innovation and the Regulation of Modern Financial Markets*, 2.2, HARVARD BUSINESS LAW REVIEW, 235-294 (2012); available at: <https://ssrn.com/abstract=1916649>, which states that they “justify more radical regulatory intervention with a view to reducing complexity within some of the more arcane corners of the global financial system” (p. 294).

⁵¹ Douglas W. Arner, Janos Nathan Barberis, Ross P. Buckley, *The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data*, 44, JOURNAL OF FINANCIAL TRANSFORMATION, 79 (2016); UNSW LAW RESEARCH PAPER, No. 63 (2016), available at: <https://ssrn.com/abstract=3044280>.

⁵² See Emily Jones, Peter Knaack, *The Future of Global Financial Regulation*, 127, GLOBAL ECONOMIC GOVERNANCE PROGRAMME WORKING PAPER, 12-15 (2017).

⁵³ With regard to card payments, it was described as an “impossible” task by Réa-Constantina Économides-Apostolidis, *La nature juridique des relations issues de l'utilisation d'une carte de crédit dans le droit des États membres de la C.E.E.*, 46-4, REVUE INTERNATIONALE DE DROIT COMPARE, 1024 (1994).

and the new Fintech models. They preferred to wait and see and allow the market to develop before regulating it. It is the tech companies who have requested regulation, a safe harbour in which to develop their business⁵⁴. The authorities act as regulators but also as catalysts for change. This stimulates the development of the new tech-based business models.

It is a matter of creating an organised digital payment system in which banks and tech companies collaborate under the supervision of the financial authorities and data protection agencies.

Unlike other financial sectors in which Fintech companies fit within the legally reserved sphere of financial activities, in the payment services sector the regulatory framework has very closely followed the evolution of the market and has covered the main services based on digital technology. A framework suitable for Fintech companies that is open to competition based on the customers' right to make use of their data is emerging. There is a trend towards a framework that is gradually and proportionally adapting to innovations based on consulting with the operators. In order to facilitate the transfer, reauthorisation channels are provided for companies that operated under a payment institution or e-money institution licence⁵⁵. Ways are being created for conversion into Fintech companies subject to the new regulations in EU Directive 2015/2366 (PSD2)⁵⁶.

The new digital services are being regulated in order to create an integrated payment market, which is an essential part of the Banking Union. It is a framework being developed with the participation of the industry in order to produce common standards that make it possible to

⁵⁴ See Asociación Española Fintech e Insurtech, *Libro Blanco de la Regulación Fintech en España* (2017), which states that “failure by the public authorities to take a proactive approach in carrying out specific actions to regulate the FinTech phenomenon would imply a clear competitive disadvantage that would translate into an outflow of capital and companies towards more secure regulatory environments” (p. 85).

⁵⁵ See, in Italy, Comitato Pagamenti Italia, *Resoconto riunione comitato pagamenti Italia*, 1 (2017), available at: https://www.bancaditalia.it/compiti/sispaga-mercati/comitato-pagamenti-italia/CPI_Resoconto_23_febbraio_2018.pdf; and, in Spain, Bank of Spain, *Instrucciones para la aportación de información relativa a los nuevos requisitos establecidos en la Directiva 2015/2366 de servicios de pago en el mercado interior (PSD2), para entidades de pago, incluidas las entidades de pago híbridas, y entidades de dinero electrónico incluidas en los registros Oficiales del Banco de España* (2018), available at: https://sedeelectronica.bde.es/f/websede/INF/VCS/Ficheros/descargar/INSTRUCCIONES_PARA_LA_APORTACION_DE_INFORMACION_DE_REQUISITOS_SEGUN_DIRECTIVA_2015_2366.pdf

⁵⁶ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

optimise investment for the benefit of consumers and the operators themselves⁵⁷. It leaves it up to the EBA, following public consultation, to draw up the regulatory technical standards (RTS) for approval by the European Commission concerning authentication of payment orders and communication between systems⁵⁸. The EBA also issues guidelines to ensure supervisory convergence⁵⁹.

Regulation seeks to facilitate innovation in a market open to competition, while preserving the market's integrity. Payment services continue to use clearing and settlement houses as infrastructure under the control of the banking authorities. These houses are public assets that guarantee the public's trust in the payment system. Innovation should be encouraged but without jeopardising the public's trust in the payment system. Decentralised systems that use blockchain technology are still in the experimentation phase. From an institutional perspective, financial innovations must respect the infrastructure that guarantees trust in the payment system⁶⁰.

The European Parliament and Commission uphold the principle of technological neutrality⁶¹. The objectives of stability of the system and investor protection are maintained. However, the search for efficiency encourages the development of Fintech. Innovation hubs and incubators are being

⁵⁷ The Bank of Italy has expressed its perplexity regarding the powers given to this group chaired by supervised companies, see Comitato Pagamenti Italia, *Resoconto riunione comitato pagamenti Italia*, 3 (2017), available at: https://www.bancaditalia.it/compiti/sispaga-mercati/comitato-pagamenti-italia/CPI_Resoconto_23_febbraio_2018.pdf

⁵⁸ Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJEU, 13 March 2018.

⁵⁹ See Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2), EBA/GL/2017/17, 12/01/2018, and Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2), EBA/GL/2018/05, 18/7/2018, inter alia.

⁶⁰ Regarding this, see Iris HY Chiu, *A new era in fintech payment innovations? A perspective from the institutions and regulation of payment systems*, 9.2, LAW, INNOVATION AND TECHNOLOGY, 190-234 (2017).

⁶¹ See European Parliament resolution of 17 May 2017 on FinTech: the influence of technology on the future of the financial sector (2016/2243(INI)), paragraph 6, available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0211+0+DOC+PDF+V0//ES>; and European Commission, *FinTech Action plan: For a more competitive and innovative European financial sector*, COM(2018) 109/2, p. 10, available at: https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf

created and experimentation is facilitated through sandboxes. These facilities must be compatible with stability and consumer protection.

Digital payment services are provided online and are based on user trust. A breakdown in trust could bring down the platforms with systemic consequences. It is all well and good to enter into dialogue with the industry but the authorities must take action by updating the legal framework so it covers the new products and services, bringing in prudential rules that protect stability and conduct rules to protect financial consumers⁶². Any company that complies with the regulatory conditions is entitled to access the market and must be able to do so simply. Promoting business activities is a task of the government. However, the financial authorities must not set economic policy or select the operators who access the market. In payment systems, companies that meet the regulatory requirements can provide information or payment initiation services. Market access should not be conditional upon filtering through a sandbox managed by the supervisor.

Convergence between banks' and tech companies' business models requires ensuring a level playing field. If they are allowed then sandbox experimentation privileges must be temporary to prevent regulatory arbitration. Regulation must be functional, taking account of the diversity of financial activities, regardless of the technology used⁶³. There are activities that are emerging with digital technologies such as crowdfunding platforms and bank data aggregators. These activities require new regulation. In order to be effective, coordination between financial supervisors⁶⁴, and

⁶² “A sandbox is where toddlers play. Adults play by rules and if you engage in banking activities, that means you are responsibly regulated in order to protect the customers” is the opinion of Maria T. Vullo

Superintendent of NY Department of Financial Services (DFS) available at: https://www.dfs.ny.gov/about/statements/st180606_exchequer_club.pdf. This was commented on in the media, for example Meng Shi, *New York Finance Watchdog 'Fiercely Opposes' Sandboxes for Fintech Firms*, 3 August 2018, available at <https://www.coindesk.com/new-york-finance-watchdog-fiercely-opposes-sandboxes-for-fintech-firms/>

⁶³ See Douglas W. Arner, Janos Nathan Barberis, Ross P. Buckley, *The Evolution of Fintech: A New Post-Crisis Paradigm?*, UNIVERSITY OF HONG KONG FACULTY OF LAW RESEARCH PAPER, 2015/047 (October 1, 2015), available at SSRN: <https://ssrn.com/abstract=2676553>, who think that “regulators have moved towards a risk-based approach where access to data is key to prudential supervision” (p. 40).

⁶⁴ See Basel Committee on Banking Supervision Sound Practices, *Implications of fintech developments for banks and bank supervisors* (February 2018), available at: <https://www.bis.org/bcbs/publ/d431.pdf>, according to which: “Given the current and potential global growth of fintech firms, global safety and soundness can be enhanced by further supervisory coordination and information-sharing where appropriate for crossborder fintech that affects banks” (p. 6). The IMF has made similar statements: Dong He, Ross Leckow, Vikram Haksar, Tommaso Mancini-Griffoli, Nigel Jenkinson, Mikari Kashima, Tanai Khiaonrong, Céline Rochon, Hervé Tourpe, *Fintech and Financial Services: Initial Considerations*, IMF

between financial supervisors and consumer protection and competition authorities, is required⁶⁵. In turn, extending the banking business into custody and management of data requires coordination between financial supervisors and the data protection authorities⁶⁶. In any case, a single contact should be provided for Fintech consultations. For digital payment services, the financial regulations are more permissive than the data regulations. It is necessary to find a way to reconcile financial innovation with appropriate protection of personal data.

The trend towards platforms makes it necessary to differentiate between different types of operators in order to define responsibilities. It is necessary to distinguish between the platform manager, the product's manufacturer and the distributor. There must be governance of the products and rules of conduct for distribution. The MiFID system provides useful architecture to regulate digital finance. New products and services must meet users' needs. The kind of customers they are aimed at and the needs they meet must be defined in the design stage. Distribution must not go beyond these limits. The platforms and other intermediaries must disclose their prices, incentives and conflicts of interest. In turn, supervisors must have the power to intervene when these precautions are breached in order to ensure user protection and market stability.

Moreover, training financial institutions' staff and the financial and digital education of users is a priority. Digital tools require progress to be made towards the knowledge society.

6. PSD2 as a universal reference model

STAFF DISCUSSION NOTE (June 9, 2017), available at: <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985>.

⁶⁵ Functional regulation requires functional supervision. In particular, the financial authorities must coordinate with the competition authorities. See A. F. Carmona, A. G. Q. Lombardo, R. Rivera, C. Pastor, J. V. García, D. R. Muñoz, L. C. Martín, *Competition issues in the Area of Financial Technology (FinTech)* (July 2018), according to whom: “*The special role of regulation in the field of financial services sends a message of caution about the appropriateness of competition policy tools as the preferred means to address every challenge*” (p. 15), available at [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU\(2018\)619027_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU(2018)619027_EN.pdf)

⁶⁶ “*Where appropriate, safety and soundness and financial stability can be enhanced by bank supervisors communicating and coordinating with relevant regulators and public authorities, such as those charged with data protection, consumer protection, fair competition and national security, to ensure that banks using innovative technologies are complying with the relevant laws and regulations*”, cf. Basel Committee on Banking Supervision Sound Practices, *Implications of fintech developments for banks and bank supervisors* (February 2018), available at <https://www.bis.org/bcbs/publ/d431.pdf>, p. 6. Regarding this, see Antonello Soro, *Fintech e Diritto*, ABI - Inaugurazione Corso di alta formazione "Fintech e Diritto", 10 May 2018, Rome, available at: <http://www.antonellosoro.it/2018/05/10/fintech-e-diritto/>

The regulation of payment services in the European Union is being used as a universal point of reference⁶⁷. It enables banks to exploit customer data through specialised third parties. The banks lack data-handling technology and the segmentation ability that tech companies have. However, they can modify their business model to become platforms that provide their customers with access to the widest range of service providers, whether payment, lending, investment or insurance services.

In 2015, payment services were the main source of income for banks in the European Union⁶⁸. The high margins point to a lack of competition. In fact, the recent innovation in the payment system has come from the tech industry. Meanwhile, the financial crisis has damaged the banks' reputation. Against this background, the European Union has opted to open up payment services to promote competition and innovation.

The emergence of new payment service providers is putting downward pressure on the banking industry's margins. Furthermore, the segmentation enabled by new technologies is a threat to traditional banking, which is coming to depend on the tech solutions offered by Fintech. Hence the overriding need to change their business model.

In the European Union, digital payment services were regulated for the first time in PSD1⁶⁹. Performance of payment transactions through telecommunication, digital or computer devices

⁶⁷ Regarding the difference of opinion in the traditional banking industry: see the amicable approach of the Euro Banking Association, *Open Banking: advancing customer-centricity, Analysis and overview*, Open Banking Working Group (2017), available at: https://www.abe-eba.eu/media/azure/production/1355/eba_open_banking_advancing_customer-centricity_march_2017.pdf; in contrast to the outright rejection of the principles of open banking in the PSD2 by the Swiss Bankers Association, *Association suisse des banquiers*, Payment Services Directive (PSD2), *Prise de position de l'ASB* (2017), available at: <http://www.swissbanking.org/fr/themes/actualite/payment-services-directive-psd2>

⁶⁸ See ECB, *Financial Stability Review November 2016 – Special features* (2016), which sets out the main sources of income: “Payment services represented the largest single category in 2015 (18%), followed by asset management (15%), distributed investment products (13%) and securities business (10%)” (p. 149), available at: https://www.ecb.europa.eu/pub/pdf/fsr/art/ecb.fsrart201611_03.en.pdf?b5d5bf6e6fb75dfc5278f6a000481fd6

⁶⁹ Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

was considered a payment service in the terms stated in the annex of PSD1⁷⁰. However, no-one was talking about Fintech back then. PSD1 was important in opening up payment services to non-bank companies. The banks lost their monopoly over this business. The legal reservation of the business was then expanded to new entrants who could use the status of "payment institution" as a passport. Many Fintech companies are currently using this status to provide digital payment services⁷¹.

In the revision of this directive by the PSD2, the approach was radically changed. PSD2 introduces new statuses for Fintech services. Tech companies can access payment service provision as a payment institution but also as a "payment initiation service provider" or an "account information service provider". It envisages Fintech services that may be provided by anyone who meets the requirements to access and provide the activity, whether tech companies, banks or other kinds of companies. It is not a scope that the PSD2 reserves for tech companies although it is true that such services were already actually being provided by some Fintech companies⁷². The banks can also provide these services under the same conditions as tech companies. In fact, information and initiation services offer banks the opportunity to expand their business. The banks can access other banks' data through the new services.

PSD2 brings about the definitive opening up of the payment market to third parties other than the banks. This directive recognises two Fintech services based on access by third-party providers to bank account data. It distinguishes between information services and payment initiation services. These providers are not authorised to capture savings from the public and open current accounts. In order to capture funds and open current accounts, they would need a bank licence. They also cannot transfer funds between bank accounts. The banks must provide the information service

⁷⁰ Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

⁷¹ For all of these, see <https://www.lemonway.com/>. This trend has been promoted by some supervisors; see <https://www.lb.lt/en/news/licence-of-a-payment-institution-issued>

⁷² This debate has also arisen in other jurisdictions. See Brian J. Hurh, Christopher M.A. Chamness, Davis Wright Tremaine, *Consumer Financial Data Aggregation & the Potential for Regulatory Intervention* (June 7, 2017), available at: <https://www.paymentlawadvisor.com/2017/06/07/consumer-financial-data-aggregation-the-potential-for-regulatory-intervention/>, who conclude that: "the regulatory approaches being developed in the EU and UK can be viewed as test cases for potential consumer financial data policy in the US."

providers with all of the available data about the customer's account, unless they are considered to be sensitive data.

The "account information service" (AIS) allows the provider to manage the information from one or more accounts that the customer holds in one or more banks. It gives the user an overall, immediate view of his/her accounting position in the banks with which he/she operates. They are aggregators of accounting information that simplify account management with new information tools.

In turn, "payment initiation services" (PIS) allow the provider to initiate payment for services from the account that the customer has in a bank. Provision of the payment initiation service makes it possible to offer accessory services in order to better manage deposits in various banks. Tech companies that sell online can save costs by initiating payments instead of depending on a bank to initiate these kinds of payments. The user can make payments online without needing to use a payment card.

Another novelty of PSD2 is the possibility of creating card-based payment instruments that allow a third party to issue cards to access the bank account that the customer holds in a bank.

7. Communication gateways (API)

"Application programming interfaces" (API) are the main mechanism used to share payment information and develop new services⁷³. They are communication gateways between the bank and the third-party providers of new services. They facilitate the use of apps. They are a set of protocols and communication tools between computer applications (interfaces), a technical foundation that makes it possible to share data securely and develop open banking. They allow better communication between the banks and their customers and third-party payment service providers. They leave it up to consumers to decide which data to share and with whom they wish to do so. They constitute a powerful tool that people must learn to use. They are used to make payments but they can be used to access all kinds of financial and non-financial services.

⁷³ See Markos Zachariadis, Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*, SWIFT INSTITUTE WORKING PAPER No. 2016-001 (June 15, 2017), available at <https://ssrn.com/abstract=2975199>, according to whom "external APIs can provide further integration with company partners and allow third parties to consume organisational data and lead to cross-selling and upselling opportunities down the line" (pp. 5 and 6).

Management of them is of strategic importance for payment service providers and, in particular, for banks.

In an open banking system, third-party payment service providers can access bank account data by assigning the customer their credentials (screen scraping) or through an API. Since the passwords are assigned, all of the customer's data can be accessed without any restrictions, except for the protections that the bank itself may develop for this kind of access. APIs are used to access the data that the interface allows. They are more secure than screen scraping, a data access system that looks set to be rejected in the European Union⁷⁴ and strictly monitored in the United States.⁷⁵

APIs have allowed the development of the major tech companies. Their use in the financial market has been delayed as it affects the trust of savers and investors and, consequently, institutions' stability. Banking infrastructures have been developed within a legal and operational framework that takes care of operational risk in order to guarantee their successful operation. The banks intend to maintain the standards in the digital environment and the financial authorities share that objective.

While the creation of the Single Euro Payments Area (SEPA) is managed by the financial industry⁷⁶, in the Fintech environment tech companies are incentivised to create standards for digital payment services⁷⁷. However, the banks maintain control over the business through

⁷⁴ See EBA, *Opinion of the European Banking Authority on the European Commission's intention to partially endorse and amend the EBA's final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2*, EBA/Op/2017/09, 29 June 2017, which concludes: "Current access approaches, often referred to as 'screen scraping', in which the TPP impersonates the consumer and has access to all the consumer's data, rather than only the data necessary to provide payment services, would not be compliant." (p. 8).

⁷⁵ See Steven T. Mnuchin, Craig S. Phillips, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, U.S. Department of the Treasury (July 2018), available at: <https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities--Nonbank-Financi...pdf>, which highlights that: "the U.S. debate seems stuck at the yet-to-be resolved issue of migrating account aggregators from screen scraping-based to more secure and efficient API-based data-sharing methodologies" (p. 27), citing Bob Hedges, *The Clearing House, Banking Perspectives: Consumer Data in an API-Enabled World* (4th Qtr. 2017), available at: <https://www.theclearinghouse.org/banking-perspectives/2017/2017-q4-bankingperspectives/articles/open-banking>.

⁷⁶ See European Payments Council, *About SEPA*, available at: <https://www.europeanpaymentscouncil.eu/about-sepa>

⁷⁷ See EY, *Global banking outlook 2018 - Pivoting toward an innovation-led strategy* (2018), which contains a revealing piece of data: "Adoption of FinTech as providers of money transfer and payment

clearing houses. In any case, self-regulation of the industry is not enough to ensure the transition to an open banking system. Leaving the setting of standards in the hands of tech companies or the banks may compromise consumers' rights. The case of Facebook and the leaking by Cambridge Analytica of the data of millions of customers shows there is a need for regulation of both tech companies and the banks with clear principles. It was a turning point in data protection, strengthening the banks' position as better custodians⁷⁸.

APIs are standardised architectures with specific characteristics in relation to their design, transmission, exchange and access to data. They are scalable, reusable and secure; in short, self-service.⁷⁹ In the financial market this system allows a security protocol to be established under the supervisors' control. It is selected by the EBA and approved by the European Commission. The financial industry uses APIs as the natural means for developing their business in the digital environment.⁸⁰

The supervisors are working in collaboration with the banks and tech companies to develop open APIs. Convergence towards common standards is being sought with a working group involving

services rose from 18% in 2015 to 50% in 2017, with 65% of consumers anticipating they would use such services at some point in future” (p. 10), available at: [https://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/\\$File/ey-global-banking-outlook-2018.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/$File/ey-global-banking-outlook-2018.pdf). According to Accenture, “Traditional payments players cannot survive without a complete overhaul of existing systems”, in *Driving the future of payments - 10 Mega Trends* (2017), available at: https://www.accenture.com/t20171012T092409Z_w/ca-en/acnmedia/PDF-62/Accenture-Driving-the-Future-of-Payments-10-Mega-Trends.pdf.

⁷⁸ See Mary Wisniewski, *Facebook's data problems have an upside for Banks*, AMERICAN BANKER (April 10, 2018), available at: <https://www.americanbanker.com/news/citibanks-app-strategy-in-the-wake-of-facebooks-data-woes>

⁷⁹ Euro Banking Association, *Understanding the business relevance of Open APIs and Open Banking for Banks*, EBA Working Group on Electronic Alternative Payments, Information Paper, 7 (2016), available at: <https://www.abe-eba.eu/media/azure/production/1380/understanding-the-business-relevance-of-open-apis-and-open-banking-for-banks.pdf>.

⁸⁰ Euro Banking Association, *Understanding the business relevance of Open APIs and Open Banking for Banks*, EBA Working Group on Electronic Alternative Payments, Information Paper (2016), available at: <https://www.abe-eba.eu/media/azure/production/1380/understanding-the-business-relevance-of-open-apis-and-open-banking-for-banks.pdf>. At the initiative of the European Commission, an Application Programming Interface (API) Evaluation Group has been set up with the following terms of reference: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-03/API%20EG%200002-18%20v1.2%20Terms%20of%20Reference%20API%20Evaluation%20Group_0.pdf

representatives of the industry, both banks and tech companies, as well as users and the financial authorities (API Evaluation Group).

Good governance of APIs is essential. There are different levels, from the requirements of internal organisation and industry standards, to universal requirements. In the United Kingdom, an industry standard for digital payments has been created through the UK Open Banking Working Group⁸¹. SWIFT is another good example⁸² that has been used as inspiration in other markets⁸³.

8. Security in digital payments

Open access to data in payment systems increases the risk of data abuse, including cybercrime. PSD2 thus introduces enhanced authentication standards. It requires two-factor authentication in accordance with the technical criteria developed by the EBA in cooperation with the ECB and approved by the European Commission⁸⁴. These regulatory technical standards (RTS) will apply from 14 September 2019. From that date on, the use of other standards will not be allowed unless they are expressly authorised. Basically, in the opinion of the EBA, it is prohibited to access customer data by taking his/her place through the screen scraping technique. The banks must establish communication channels that comply with these standards.

The RTS regulate both the identification of providers and user authentication, verifying their identity and the authorisation or approval of transactions. Enhanced authentication includes three elements: firstly, something that the customer knows (password/PIN); secondly, something that

⁸¹ There is a wide range of initiatives to create API standards to facilitate digital payments. See Euro Banking Association, *Understanding the business relevance of Open APIs and Open Banking for Banks*, EBA Working Group on Electronic Alternative Payments, Information Paper, 12-14 (2016), available at: <https://www.abe-eba.eu/media/azure/production/1380/understanding-the-business-relevance-of-open-apis-and-open-banking-for-banks.pdf>

⁸² Described in Markos Zachariadis, Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking* (June 15, 2017).

⁸³ See Hong Kong Monetary Authority (HKMA), *Consultation Paper on Open API Framework for the Hong Kong Banking Sector*, 7 (2018), available at: <http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/20180111e1.pdf>

⁸⁴ Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJEU, 13 March 2018.

the user has (mobile phone/device); and, lastly, something inherent to the user (fingerprint/facial recognition)⁸⁵.

The EBA has established exemptions to the application of enhanced authentication⁸⁶. Transactions for a low amount, that are low-risk or have trusted beneficiaries are excluded. There are also exclusions for operational security reasons, such as preventing queues at toll booths. It is a flexible system that seeks to strike a balance between security and ease in payments. It is necessary to avoid the blocking of services that were previously being used. Transactions that are classified as low-risk may be exempt from enhanced authentication. A list of trusted beneficiaries to whom enhanced authentication is applied may be created; this white list must be confirmed by the service user. This list may turn into a hotchpotch if the user can include card payments through major platforms⁸⁷.

Control is maintained by the account managing bank, which may deny access to the account by the information service or payment initiation provider “*for objectively justified and duly evidenced reasons*”⁸⁸.

Changing the banking model is not risk-free. The raw material is switching from money to data. Risks arise from the use, or rather abuse, of customer data. It is no accident that PSD2 has come at the same time as the General Data Protection Regulation (GDPR)⁸⁹. Leaking of data without the data subject's consent is the main risk involved in the new digital payment services. It could give rise to cases that result in heavy fines. The GDPR has become the regulation of reference for

⁸⁵ Mounaim Cortet, Tom Rijks, Shikko Nijland, *PSD2: The digital transformation accelerator for banks*, 10.1, JOURNAL OF PAYMENTS STRATEGY & SYSTEMS, 20 (2016); Mark Hartley, *Banking heroes: the IT department* (2018), available at: <https://www.bankifi.com/blog/banking-heroes-the-it-department>

⁸⁶ See Eduardo Avendaño, David Pérez Lázaro, Bárbara Queizán, *Medios de pago, seguridad e identidad digital*, 149, PAPELES DE ECONOMÍA ESPAÑOLA, 127-143 (2016).

⁸⁷ José Luis Lorente Howell, *Exenciones a la autenticación reforzada en la Directiva de Services de Pago*, 930, ACTUALIDAD JURÍDICA ARANZADI, 7 (2017).

⁸⁸ Art. 68.5 PSD2.

⁸⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Fintech companies⁹⁰. One of the main risks the banks face comes from data protection infringements following the entry into force of the GDPR in a shared data environment.

PSD2 is a system that combines market freedom with enhanced security in which the EBA is the authority in the system with the power to create technical regulations that are essential to ensure its smooth operation, such as secure customer authentication. It is a maximalist directive that leaves little room for manoeuvre by national legislatures. However, there are grey areas concerning the protection of customers' personal data, which calls into question the compatibility of PSD2 with GDPR⁹¹.

In PSD2, in the event of fraud in the use of data, the account managing bank remains liable. Hence the need to maximise security. For tech companies, the relevant aspect is providing the service to capture the customer. For the banks, security comes first⁹².

All institutions that hold or receive customer data related to the provision of payment services must maintain the same security standards. They must be authorised institutions. Inspection and supervision of these institutions must be performed by the banking authority. In Australia it has been proposed that control of data in an open banking system should be performed by several authorities under the leadership of the Competition and Consumers Commission with opinions contributed by the sector-specific authorities⁹³.

⁹⁰ Ryan Browne, *Zuckerberg says Facebook has 'always shared' the values of Europe's new data law*, CNBC (May 24, 2018), available at: <https://www.cnn.com/2018/05/24/zuckerberg-facebook-has-always-shared-values-of-europes-gdpr.html>. Darcy Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, Jason Potts, Darcy Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, Jason Potts, *Some Economic Consequences of the GDPR*, (May 23, 2018), available at <https://ssrn.com/abstract=3160404>, according to whom: “*This far-reaching regulation creates incentives for new financial products in an effort to mitigate the operational risk that data collectors and processors will face*”; and furthermore, it “*creates a security that can be purchased or sold*”.

⁹¹ See Gautier Calomne, Johan Klaps, *Rapport Projet de Loi relative relatif au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement*, 1 March 2018, available at: <http://www.dekamer.be/FLWB/PDF/54/2896/54K2896002.pdf>

⁹² Steve Mansfield-Devine, *Open banking: opportunity and danger*, 10 COMPUTER FRAUD & SECURITY, 8-13 (2016), according to whom “*the more doors you open, the bigger the attack surface*” (p. 10).

⁹³ Australian Government, *Review into Open Banking: giving customers choice, convenience and confidence*, 16-17 (2017), available at: <https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-For-web-1.pdf>

Within this security framework, the banking industry plays the leading role since it must create secure infrastructure for others to work with⁹⁴.

9. Conclusions

User trust is necessary in order to ensure the smooth operation of the payment system in the Fintech environment too. Accordingly, the regulators' main objective is security. Innovation is thus being promoted within a regulated framework.

Supervisors must take a functional approach with technological neutrality. The same rules must apply and the same approach must be taken by the supervisor to the same activities and the same risks. There must be consistency in how similar risks are handled⁹⁵. Technological neutrality is applied based on the principle of proportionality, which provides a degree of flexibility for technological new entrants. A degree of experimentation (sandbox) is allowed in this framework until the supervisors familiarise themselves with the new products and services. It is necessary to ensure fair competition with the application of the same rules to maintain consumer protection and preserve market integrity. The objective is to reconcile innovation with the security and stability of the financial system.

In the new payment system, communication gateways are used for third-party service providers through open APIs, although the banks maintain a degree of control in order to preserve security and comply with data protection regulations. Banking is being opened up to third parties and the model of financial distribution is changing. There is a risk of disintermediation but also an opportunity to expand the business. Conduct restricting free competition has not been detected yet but it is necessary to supervise the large banks and tech companies to ensure they do not abuse their market power over the data of payment service users in order to prevent new operators from entering the market.

Growing technical complexity increases the risks posed to security in the payment system. Operational risk is rising as a consequence of opening up databases to third parties. In turn, artificial intelligence is threatening to convert algorithms into black boxes that are impossible to

⁹⁴ Michael Salmony, *Rethinking digital identity*, 12.1, JOURNAL OF PAYMENTS STRATEGY & SYSTEMS, 54 (2018).

⁹⁵ European Banking Authority, *The EBA's Fintech Roadmap. Conclusions from the consultation on the EBA's approach to financial technology (Fintech)*, 10 (2018), available at: <https://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf>

control. It is necessary to enhance prevention and management of operational and security risks. In order to facilitate control, the authorities must be informed about incidents that affect payment security.

In the European Union, payment service providers, including payment initiators and information aggregators, must use enhanced identification systems in their relations with their customers. In turn, users must be aware of the consequences of consenting to the transfer of their data. They must be equipped and trained to use these communication channels.

New facts, new law. Given the innovation affecting payment services, the European Union's regulations are right to combine financial regulation with data protection. These force the banks to share customer data with tech companies in a secure manner. Customers can make use of their data and doing so facilitates development of the market.