THE OPEN BANKING MOVEMENT AND THE ACCESS TO ACCOUNTS RULE: CHALLENGES FOR COMPETITION AND DATA PROTECTION LAW

Alessandro Palmieri[1]

DOI: https://doi.org/10.24040/pros.13.11.2020.svp.222-232

Abstract

The global development of open banking regulations and initiatives, while promising benefits to individuals and small businesses, raises also several concerns. This entry, focusing on the European Union experience, addresses some critical issues not only in respect to the defence of consumers' economic interests, but also, and mainly, with regard to the safeguard of customers' personal data and the maintenance of an adequate level of competition in the relevant markets. The author advocates a revision of the existing protecting devices or, alternatively, the creation of new mechanisms, more suitable to ensure a high level of protection for the interests at stake.

Keywords

Open banking, payment services, consumer protection, competition, data protection

Introduction

The open banking movement is at the centre of a worldwide debate. Several legislatures, at the national as well as the supranational level, have taken significant steps towards implementing an efficient open banking regime, susceptible of being, as a first approximation, described as a system under which banks open up their application programming interfaces (APIs) for third parties[2].

The process of implementation of open banking raises many legal questions, related to different branches of law. Indeed, since the first stage of its development, open banking,

[1] Prof. Dr. Alessandro Palmieri, PhD., University of Siena, Department of Law.
[2] According to P. Gupta and T.M. Tham, *Fintech. The New DNA of Financial Services*, de Gruyter, 2019, 157, consists in the «adoption of common standards for collaboration between banks and other players within the banking ecosystem».

alongside the expected benefits, has revealed critical issues, which demand the attention of academics and other experts from various areas of law. In this context, one may come across issues that pertain to private law: more specifically, focus shall be put on consumer protection, personal data privacy and the safeguard of competition. A large part of the difficulties stem from one of the core features of the open banking system, that is to say from the "access to account rule", according to which financial institutions are obliged to allow third parties to obtain customers' account data on the basis of customers' consent.

Open banking as a global phenomenon: a window on non-European experiences

As it has been pointed out in the relevant literature, open banking "is proving to be a global phenomenon"[3]. Before concentrating on European Union, it seems useful to conduct a survey of non-European experiences.

It is extremely remarkable the way Australia has dealt, and keeps on dealing, with open banking, in the framework of a more ambitious project that aims at enhancing an open-data landscape. In July 2020, the Australian Consumer Data Right Act came into force, which pursues the goal of improving competition and choice, as allows that transaction data, customer data and product data can be communicated with third party comparison sites to increase the consumer's negotiation power. The scope of this piece of legislation is very broad: in the initial stage, it is applicable only in the banking sector; then it will apply to the energy and telecommunications sectors, before including gradually other industries on a sector-by-sector basis. It is also of interest what is taking place in Brazil. In May 2000, the Central Bank of Brazil (Banco Central do Brasil) has issued a regulation on the implementation of open banking. Like similar attempts to govern the phenomenon, the said regulation – which defines open banking as a standardized sharing of data and services through the opening and integration of systems – aims at encouraging innovation, promoting competition, and increasing the efficiency of the national financial system.

Other legal systems are preparing the adoption of the open banking paradigm. One of these is Canada where, in June 2019, the Senate Committee on Banking, Trade and Commerce

[3] See, for instance, B. Regnard-Weinrabe and J. Finlayson-Brown, *Adapting to a changing payments landscape*, in J. Madir (ed.), *FinTech. Law and Regulation*, Edward Elgar, 2019, 41.

asked the Government to take immediate steps to initiate an open banking framework. More recently, in January 2020, the Advisory Committee on Open Banking, appointed by the Ministry of Finance, determined that the benefits of open banking outweigh its cost. In its report the Committee observed that a robust consumer-directed framework: 1) could give consumers greater control of their information; 2) could support a more innovative and competitive sector by setting rules and protections around data use and requiring data to be transferred in a more secure form. After the publication of this report, a new phase commenced in the design of an open banking regulatory framework. Currently the focus is on determining how regulators and the financial sector can mitigate data security and privacy risks. Something noteworthy is happening in the United States where, as of today, consumers' access to financial data sharing has been largely dependent on private-sector efforts. Indeed, Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (passed in the aftermath of the financial crisis of 2008) provides that, subject to rules prescribed by the Bureau of Consumer Financial Protection (CFPB), a consumer financial services provider must make available to a consumer information, in its control or possession, concerning the consumer financial product or service that the consumer obtained from the provider. This provision, which dates bakes to 2010, has never been implemented. But, on 22 October 2020, the CFPB has announced its intention to regulate open banking, issuing an advanced notice of proposed rulemaking.

It shall be noted that other countries – including India, Japan, Singapore and South Korea – still rely on market mechanisms as levers to support the growth of open banking and the effectiveness of data sharing measures.

The access to account rule in the EU system

European Union is widely regarded as the frontrunner of the above said global tendency, due to the fact that its decisive move to reach the mentioned goal dates back to 2015, when the Directive (EU) 2015/2366, on payment services in the internal market (known as "PSD2") was enacted. And, more recently, EU seems to have taken the lead in the ambitious road towards open finance. As a matter of fact, in the context of the "Digital Finance Strategy", launched in September 2020, the European Commission announced that, by 2024, the EU should have an open finance framework in place, in line with the EU Data Strategy, the upcoming Data Act,

and Digital Services Act. The concept of open finance goes beyond open banking because it involves the sharing and use of customer-permissioned data by banks and third-party providers to create new services.

One of the crucial factors in the context of PSD2 is the "access to accounts rule" (often labelled as "XS2A").

Speaking of this rule, several provisions of the Directive are relevant. First, one has to take into account Article 36 ["Access to accounts maintained with a credit institution"] which states that: "Member States shall ensure that payment institutions have access to credit institutions' payment accounts services on an objective, non-discriminatory and proportionate basis. Such access shall be sufficiently extensive to allow payment institutions to provide payment services in an unhindered and efficient manner. The credit institution shall provide the competent authority with duly motivated reasons for any rejection".

Then, one encounters two other provisions devoted, respectively, to payment initiation services (Article 66, entitled "Rules on access to payment account in the case of payment initiation services") and to account information services (Article 67, entitled "Rules on access to and use of payment account information in the case of account information services").

According to paragraph 1 of Article 66, "Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services […]. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online". The supply of the payment initiation service inevitably requires that the third-party providers shall have access to some of the payment service user's data, and the ability to store them. But, in this regard, the EU legislature has introduced some limits; the payment initiation service provider is prevented from: 1) storing sensitive payment data of the payment service user (paragraph 3, lett. e); 2) requesting from the payment service user any data other than those necessary to provide the payment initiation service (paragraph 3, lett. f); 3) using, accessing or storing any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer (paragraph 3, lett. g)[4].

Furthermore, according to paragraph 1 of Article 67, "Member States shall ensure that a payment service user has the right to make use of services enabling access to account

[4] Axccording to B. Geva, *Payment Transactions under the E.U. Second Payment Services Directive – An Outsider's View*, 54 Tex. Int'l L.J. 211, 220 (2019), regulatory standards favor the indirect acces mode, where the Account Servicing Payment Service Provider provides the Payment Initiation Services Provider (PISP) account access through a dedicated application interface, because this mode is capable of limiting the data accessed by the PISP to only what is required for the provision of the service

information […]. That right shall not apply where the payment account is not accessible online". In addition, paragraph 2, lett. a), specifies that the account information service provider shall "provide services only where based on the payment service user's explicit consent".

Concerns for consumers' interests, data protection and competition in the marketplace

The access to account rule could have an adverse impact not only on the economic interests of consumers and other weak parties (such as microenterprises), but also on customers' data protection as well as on the competitiveness of the market as a whole.

Among the most serious dangers, one has to mention unauthorized payments or transactions made without the account holder's permission and defective payments or transactions, requested by the customer but wrongly processed by the providers involved. Concerns have also been raised about the information obligations that payment service providers should fulfil toward payment service users in respect to the payment service contract and payment operations. Regardless of the fact that the EU legislation sets out a package of rules designed to foster transparency, improving the information requirements, especially devoted to framework contracts and payment transactions subject to such contracts, which are of greater economic importance than singular payment transactions [arts. 38 et seq. PSD2], these rules must be placed in their proper position in the general framework of consumer protection law.

However, the specific problems affecting the consumer as payer have been addressed in 2019 by European Court of Justice in the *Verein für Konsumenteninformation* judgment[5]. On that occasion, the ECJ was asked to clarify the scope of provisions that were not immediately linked to consumer protection, since they were instead related to the technical and business requirements for credit transfers and direct debits [Regulation 260 of 2018]; nevertheless, it provided a favourable interpretation for consumers, imposing a ban on discrimination between different classes of purchasers. If this judgment proves to be the expression of a lasting trend, this will lead to enhance the protection of payers. As I have noted elsewhere, usually consumers in the digital environment combine the roles of buyers and payers; so, making stronger the

[5] ECJ 5 September 2019 [ECLI:EU:C:2019:673].

position of the payers will likely result in an overall enhancement of the digital consumers' economic welfare.

Other crucial issues are raised by the intersection between the open banking business model and data protection principles. Several risks are related to the processing of personal data connected to the provision of the services in this new business environment. It seems necessary to eliminate the inconsistencies between the sector-specific rules and the provisions set out by the General Data Protection Regulation (GDPR). Useful elucidations are offered in the "Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR", adopted by the European Data Protection Board (EDPB) on 17 July 2020. In particular, in that document, the EDPB expressed its view on the nature of the explicit consent of the payment service user required by some significant provisions of PSD2, specifying that consent under PSD2 is different from consent under GDPR, because the first one is deemed to be an additional requirement of a contractual nature.

Under the GDPR, consent serves as one of the six legal grounds for the lawfulness of processing of personal data. Article 4 (11) of the GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". These four conditions –freely given, specific, informed, and unambiguous– are essential for the validity of consent. The EDPB has recently specified (in its Guidelines 05/2020 on consent under Regulation 2016/679), that consent can only be an appropriate lawful basis if a data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. Moreover, according to Article 9 of the GDPR, consent is one of the exceptions from the general prohibition for processing special categories of personal data. However, in such case the data subject's consent must be 'explicit'. This means that the data subject must give an express statement of consent for specific processing purpose or purposes. Although the consent mentioned in PSD2 is not a legal ground for the processing of personal data, this consent is specifically related to personal data and data protection, and ensures transparency and a degree of control for the payment service user. It is interesting to observe that the EDPB added that the payment service user must be able to choose whether to use the service and cannot be forced to do so. Therefore, the consent under PSD2 must be a freely given consent too.

In terms of data protection law, it has to be recalled also the principle of data minimisation, according to which third-party providers should collect only personal data necessary to provide the specific payment services requested by the payment service user. Since financial data may contain references to all aspects of a data subject's private life, it is necessary to find out the best strategies that can be developed to avoid data breaches (just think of the consequences of giving untrusted parties access to log-in credentials) or, when a breach occurs, to grant an effective remedy to persons whose fundamental rights have been violated.

Furthermore, one has to consider that the judgment of the ECJ in the *Facebook Ireland and Schrems* case[6] (which has declared invalid the Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-US Privacy Shield) may influence the processing of personal data carried out for the purposes of open banking, since a meaningful number of Account Information Service Providers and Payment Initiation Services Providers, are located outside the EU. The ECJ has made clear that GDPR provisions apply to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.

Although one of the purposes of the rules enacted at the European level is to increase competition and openness between banks and non-banking institutions, antitrust issues may arise from the business conduct of the various operators. It is particularly important to make competition work in a sector where some players (namely, Big-Tech firms), leveraging on their skills in the field of data analytics, may acquire a dominant position, which in the end could result in a welfare loss for consumers.

[6] ECJ 16 July 2020 [ECLI:EU:C:2020:559]. In that circumstance, the Court held also that Article 46(1) and Article 46(2)(c) of the GDPR «must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation». On the *Facebook Ireland and Schrems* judgment, see M. Rotenberg*, Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*, in *European Law Journal*, 2000, vol. 26, 1-2, 141-152; A. Chander, *Is Data Localization a Solution for Schrems II?*, in *Journal of International Economic Law*, 2000, vol. 23, 3, 771-784.

In the light of the provisions concerning the access to, and the use of, data relating to online payment accounts, many aspects have to be clarified from a competition law point of view: among the others, the definition of the relevant markets; the identification of the dominant entities; the relationship with the essential facility doctrine.

With respect to this specific point, many observers are fearful about the effects of the entry into the market of the so-called Big-Tech giants. An interesting proposal of reform, which aims at rebalancing power relations between the different parties, is centred in the idea that a reciprocity clause shall be added to the rules currently in force, so that not only third-party providers would be able to access bank customers' data, but also banks should be entitled to access all data stored by the said providers pertaining to the same customers[7].

Specific tools have to be designed in order to prevent the monopolization of the market by Big-Tech firms, which may leverage on their ability to tailor their services around customers' needs, to exploit economies of scope, and to cross-subsidise their services with the ones they offer in other markets. The competition problems encountered in the financial sector need to be inscribed in the framework of the more general debate around access to data in the digital sphere.

Civil liability rules can play a significative role in this context, to the extent that they are able to compensate those who have sustained losses as a result of unlawful conducts of banks, financial institutions, Account Information Service Providers and Payment Initiation Services Providers, as well as to deter further infringements.

Conclusion

According to an article recently published in is an international journal of technology law, the analysis of PSD2, and of the Regulatory Technical Standards adopted by the Commission, shows that the goal to develop the market for payment services has a higher priority; security and privacy are ultimately subordinate[8]. Analogous concerns can be raised with respect to the safeguard of a fair and vibrant competition in the relevant markets.

[7] F. Di Porto, G. Ghidini, ''I Access Your Data, You Access Mine'': Requiring Data Reciprocity in Payment Services, in International Review of Intellectual Property and Competition Law - IIC, 2020, 51, p. 307-329.
[8] See P.T.J Wolters, B.P.F. Jacobs, *The security of access to accounts under the PSD2*, in *Computer Law & Security Review*, 2019, 35, p. 29-41.

Since we are already in the 'open banking age' (at least in an early stage of it), and we are approaching the 'open finance age', scholars and other experts are called to explore new paths in order to minimise the mentioned risks, trying to adapt the existing protecting devices or to create new mechanisms, more suitable to face such important challenges as we are doing nowadays. These tools should increase the overall security of digital transactions and ensure a high level of protection to consumers and other vulnerable parties.

BIBLIOGRAPHY

ARNER D.W., ZETZSCHE D.A., BUCKLEY R.P., WEBER R.H.: Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II, in Standard Journal of Law Business and Finance, 2020, vol. 25, 245-288.

BORGOGNO O., COLANGELO G.: Data, Innovation and Competition in Finance: The Case of the Access to Account Rule, in European Business Law Review, 2020, 31, no. 4, 573-610.

BORGOGNO O., COLANGELO G.: The data sharing paradox: BigTechs in finance, May 28, 2020, available at SSRN: https://ssrn.com/abstract=3591205 or http://dx.doi.org/10.2139/ssrn.3591205 (forthcoming in European Competition Journal).

BURDON M., MACKIE T.: Australia's Consumer Data Right and the Uncertain Role of Information Privacy Law, in International Data Privacy Law, 2020, 10(3), 222-235.

CHANDER A.: Is Data Localization a Solution for Schrems II?, in Journal of International Economic Law, 2000, vol. 23, 3, 771-784

CIRAOLO F.: Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti", in Rivista di diritto bancario, 2020, 611-650.

DE PAOLI D.: PSD2 e privacy, in M.C. Paglietti, M.I. Vangelisti (eds.), Innovazione e regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2, Roma TrE-Press, 2020, 147-151.

DI PORTO F., GHIDINI G.: ''I Access Your Data, You Access Mine'': Requiring Data Reciprocity in Payment Services, in International Review of Intellectual Property and Competition Law - IIC, 2020, 51, 307-329.

GAMMALDI D., IACOMINI C.: Mutamenti del mercato dopo la PSD2, in Maimeri F., Mancini M. (eds.), Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute

e rivoluzione digitale, Quaderni di Ricerca Giuridica della Consulenza Legale, Banca d'Italia, 2019, no. 87, 123-142.

GAUCI R.: Is Europe a Good Example of Open Banking?, in S. Chishti, T. Craddock, R. Courtneidge, M. Zachariadis (eds.), The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries, Wiley, 2020, 86-87.

GEVA B.: Payment Transactions under the E.U. Second Payment Services Directive – An Outsider's View, 54 Tex. Int'l L.J. 211 (2019).

GIROMPINI D.: PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche, in Bancaria, 2018, no.1, 70-73.

GUPTA P.T., THAM M.: Fintech. The New DNA of Financial Services, de Gruyter, 2019.

KOTTAYIL N.M.: Consumer Security and Liability Model for Open Banking, in International Journal of Trend in Research and Development, 2020, 7(4), 230-232.

LEONG E.: Open Banking: The Changing Nature of Regulating Banking Data - A Case Study of Australia and Singapore, in Banking & Finance Law Review, 2020, 35.3, 443-469.

MELI V.: Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento, in M.C. Paglietti, M.I. Vangelisti (eds.), Innovazione e regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2, Roma TrE-Press, 2020, 135-145.

MILANESI D.: A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States, in TTLF Working Papers, 2017, No. 29.

O'DONNELL B.: Data and Privacy in the Next Decade, in King M.R., Nesbitt R.W., The Technological Revolution in Financial Services: How Banks, Fintechs, and Customers Win Together, University of Toronto Press, 2020, 116-128.

PACKIN, N.G.: Show Me the (Data About the) Money!, available at SSRN: https://ssrn.com/abstract=3620025 (forthcoming in Utah Law Review).

PERNG B.J.: Align Open Banking and Future-Proof RegTech for Regulators and Third-Party Providers to Deliver the Optimal Consumer Convenience and Protection, in Barberis J., Arner D.W., Buckley R.P. (eds.), The RegTech Book, he Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation, Wiley, 2019, 89-92.

RAJARETNAM T., YOUNG A.: The promise of an open data economy in Australia: legislating open banking, in Computer and Telecommunications Law Review, 2020, 26(4), 83-90.

REGNARD-WEINRABE B., FINLAYSON-BROWN J.: Adapting to a changing payments landscape, in J. Madir (ed.), FinTech. Law and Regulation, Edward Elgar, 2019, 22-48.
ROTENBERG M.: Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection, in European Law Journal, 2000, vol. 26, 1-2, 141-152
STIEFMUELLER C.M.; Open Banking and PSD 2: The Promise of Transforming Banking by 'Empowering Customers', in Spohrer J., Leitner C. (eds.), Advances in the Human Side of Service Engineering. AHFE 2020. Advances in Intelligent Systems and Computing, vol 1208. Springer, 2020, 299-305.
WOLTERS, P.T.J., JACOBS, B.P.F.: The security of access to accounts under the PSD2, in Computer Law & Security Review, 2019, 35, 29-41.
ZACHARIADIS M.: How 'Open' is the Future of Banking? Data-Sharing and Open Data Frameworks in Financial Services, in King M.R., Nesbitt R.W. (eds.), The Technological Revolution in Financial Services: How Banks, Fintechs, and Customers Win Together, University of Toronto Press, 2020, 129-157.
ZETZSCHE D.A., ARNER D.W., BUCKLEY R.P., WEBER R.H.: The Evolution and Future of Data-Driven Finance in the E.U., in Common Market Law Review, 2020, vol. 57, 331-360.