Haut Comité Juridique de la Place financière de Paris

REPORT ON THE REVISION OF THE PAYMENT SERVICES DIRECTIVE 2 (PSD2)

of the Haut Comité Juridique de la Place financière de Paris

September 2023

TABLE OF CONTENTS

INTRODUCTION

In a period of rapid and continuous growth in dematerialised payment technologies, such as contactless payment technologies, tokenised payment cards (X-pay solutions, offered by Apple, Samsung, Google, etc.), stable coins and, soon, central bank digital money,[1] the need to review the current legal framework for payment services laid down by Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market ("**PSD2**")[2] is necessary, despite its entry into force just 4 years ago.

In 2007, the aim of the first Payment Services Directive ("**PSD1**") was to create a "single payment area" within the European Union. Seventeen years on, this objective is still being implemented. On 24 September 2020, as part of its digital package, the European Commission unveiled its strategies for digital finance[3] and retail payments[4], including a comprehensive review of the application of PSD2 in the light of market and technological developments. This initiative aims to address several different issues, including new market players (such as fintechs and Big Techs) offering payment services in addition to their business or other companies adopting new technologies to implement payment solutions such as digital wallets or contactless payments. At the same time, consumer habits have also changed, with increased use of online payment and alternative means of payment to the traditional bank card in particular with smartphones and NFC technology. The Commission is keen to ensure that the scope, exclusions and definitions remain adequate to ensure regulation of these actors, fair competition and security for payment service users[5],

---

1 Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC.

2 The same applies to Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC ("**EMD2**"), available here.

3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a digital finance strategy for the EU, 24 September 2020, available here.

4 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on retail payments, 24 September 2020, available here.

5 European Commission, call for contributions, 10 May 2022, available here.

objectives already identified in the 2013 PSD2 proposal.[6] The Commission also intends to step up the fight against payment fraud and make it more effective, by re-examining the conditions for authenticating the payment service users who send a payment order to their payment service provider ("**PSP**").[7] Finally, the review of PSD2 also aims to improve access to payment account data and make international payments cost-effective and transparent.[8]

In October 2021, the European Banking Authority ("**EBA**") was asked to give its opinion on the revision of PSD2, which was made public on 23 June 2022. This opinion, encouraging the Commission to revise PSD2, sets out over 200 proposals to contribute to the development of the single market for retail payments in the European Union ("**EU**") and to ensure a harmonised and consistent application of legal requirements across the EU. In particular, the EBA's proposals seek to enhance competition, facilitate innovation, protect consumers' funds and data, encourage the development of user-friendly services and prevent the exclusion of the most disadvantaged from access to payment services, as well as ensuring harmonised and consistent application of legal requirements across the EU.[9] At the same time, the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union ("**DG FISMA**")[10] has also been examining the conditions for implementing PSD2 and how it could be further improved. It published a report at the beginning of 2023[11], highlighting the development of technologies and the growing demand for faster, more reliable and less expensive payment solutions. PSD2 has included two new services in the list of payment services (account information services and initiation of payment transactions), but many other so-called technical service providers are now playing a much more substantial role in the payment services value chain. This is the case even though they remain outside of PSD2's scope, due of the definition of technical service providers which creates a particularly porous boundary between technical services and payment services. This can be observed with the "tech giants" offering

---

6 Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, p. 2, available here.

7 *Ibid.*

8 *Ibid.*

9 EBA, "*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*", EBA/Op/2022/06, 23 June 2022, available here .

10 *Financial Stability, Financial Services and Capital Markets Union Directorate - General.*

11 "*A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*", FISMA/2021/OP/0002. The report is available here.

to pay for purchases directly with a smartphone, such as Apple, Samsung or Google, which offer "X-pay" type payment solutions.

The inclusion of new technologies (blockchain, cloud, digitisation/tokenisation, digital assets and currencies, etc.) and related services and activities in European legislation (such as the recent adoption of the DORA[12] and MiCA[13] regulations, for example) is placing older texts such as PSD2 and EMD2 under scrutiny.

Furthermore, the direction of modern European legislative texts (tending towards more regulations and fewer directives)[14] advocated by the de Larosière Report in response to the major financial crisis of 2008,[15] and the aforementioned reports argue in favour of greater harmonisation of the legal framework for payment services in the various Member States. The elevation of PSD2 to a regulation[16] should be a solution consistent with this development. Similarly, it is also necessary to harmonise the approaches of the various supervisory authorities involved in payment services, to ensure that its provisions are applied in the same way throughout the EU. It has been observed that, all too often, the approaches of the competent authorities in the Member States diverge and lead to different supervisory practices that are detrimental to legal certainty and fair competition between Member States. The multi-jurisdictional analyses carried out as part of this

---

12 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital business resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, available here ("**DORA Regulation**").

13 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, available here ("**MiCA Regulation**").

14 Initiated by the "***CRA* Regulation**" (Regulation (EC) No. 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies) available here, then "**MAR**" (Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) available here, "**Benchmark**" (Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks for financial instruments and contracts or to measure the performance of investment funds) available here, "**Prospectus**" (Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus) available here; more recently, MiCA, "**Pilot Regime**" (Regulation (EU) 2022/858 of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (DLT), available here)

15 *"Report of the High-Level Group on Financial Supervision in the EU*, chaired by J. de Larosière, 25 February 2009, spec. §109 and Recommendation 10, available here.

16 Or, failing that, some of its provisions, as in the banking sector with the CRD/CRR package (Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 and Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013).

report provide some illustrations of this, which complement those of the EBA and the European Commission/DG FISMA.[17]

Against this background, the *Haut Comité Juridique de la Place de Paris* ("**HCJP**") set up a working group in May 2022 to consider and examine the changes it wanted to be made in PSD2, in anticipation of an imminent legislative proposal from the Commission. The HCJP aimed to present concrete recommendations. The composition of this working group has sought to ensure the broadest possible representation of actors in the payment services market in France. Representatives of credit, payment and e-money institutions, professional organisations and the French Prudential Supervision and Resolution Authority (*Autorité de contrôle prudentiel et de résolution*) ("**ACPR**"), as well as academics, specialist lawyers and financial authorities, have been invited to contribute their expertise to the group's work.[18]

Given the variety of topics and the risk of dispersing itself, the working group decided to concentrate on a limited number of subjects, namely:

- replacing PSD2 with a regulation;
- the merger of PSD2 with the Electronic Money Directive (EMD2);
- the territorial scope of the PSD2;
- the question of whether the business of collecting funds on behalf of third parties should be subject to the PSD2;
- certain exclusion regimes from the material scope of PSD2 (in particular, technical service providers, intra-group exclusion, etc.);
- the concept of the payment account;
- the PSP liability regime; and
- access granted to account information service providers ("**AISP**") and payment initiation service providers ("**PISP**") to data held by PSPs managing payment accounts.

Given the diversity of the members of the working group, certain sparked debates that occasionally failed to reach a consensus on recommendations. This report

17 See footnote no. 9 and 10 above.

18 The composition of the working group is shown in Appendix II.

acknowledges and reflects these differences. However, the report does successfully articulate 21 recommendations.

In order to highlight the differences in transposition of PSD2 or supervisory practices in the Member States, multi-jurisdictional analyses were carried out on certain subjects.[19] These analyses made it possible to compare the different regulatory and legislative approaches and to take account of the approaches adopted by other Member States to enrich the working group's reflections.

Meanwhile, on 28 June 2023, the Commission unveiled its plans to reform PSD2 in the form of a "package" comprising a proposal for a directive on payment services and electronic money services ("**PSD3 Proposal**")[20] and a proposal for a regulation on payment services ("**PSR Proposal**")[21] , following the example of the CRD/CRR package ("**PSD3/RSP Package**"). While the Regulation contains the rules governing the provision of payment services, the Directive concentrates on those governing access to the profession and the supervision of institutions. Incidentally, the PSD3/PSR Package merges the previous texts (PSD2 and EMD2) governing payment services and electronic money. On the same day, the Commission also unveiled its proposal on the digital euro.[22] In this respect, it is interesting to note that these different texts are linked since, on the one hand, the definition of "funds" contained in PSD2 is amended to include a reference to central bank money issued for retail payment purposes,[23] which includes the digital euro[24]. It should also be noted that, since they are treated as electronic money under the MiCA Regulation[25], electronic money tokens necessarily fall within the definition

19 Multi-jurisdictional analyses are provided in Appendix III.

20 Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the internal market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, COM(2023) 366 final, available here.

21 Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010, COM(2023) 367 final, available here.

22 Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, COM(2023) 369 final, available here, supplemented by a proposal for a Regulation of the European Parliament and of the Council on the provision of digital euro services providers incorporated in Member States whose currency is not the euro, COM(2023) 368 final, available here..

23 See Article 2(23) of the Proposed PSD3 and Article 3(30) of the Proposed PSR Regulation.

24 Recital 15 of PSD3 Proposal.

25 Article 48(2) MiCA Regulation.

of funds[26]; and secondly, digital euro will be distributed by the PSPs with which the digital euro payment accounts must be opened.[27]

The summary of the HCJP's recommendations, which appears after the introduction to this report, indicates whether or not the PSD3/PSR Package is in line with these recommendations.

Finally, to make this report easier to read, a glossary of the defined terms, abbreviations and acronyms used is included in Appendix I of this report.

[26] Recital 16 of PSD3 Proposal.

[27] Article 2(5) of the proposal on the digital euro.

SUMMARY OF RECOMMENDATIONS

Replacing the Directive with a Regulation

Recommendation No. 1: The HCJP recommends that the Directive be replaced by a Regulation.

PSD3/PSR Package: the Commission's proposal is partly in line with this recommendation, since part of PSD2 is contained in the PSR Proposal, similar to the CRD/CRR package.

PSD2 and EMD2 merger

Recommendation No. 2: The HCJP recommends the revision of the concept of electronic money, not only because the current definition remains abstruse, but also so that it can be used for the innovations currently underway, in particular concerning crypto-assets, but more broadly the new "payment value chains".

PSD3/RSP Package: the Commission's proposal does not contain any provisions reflecting this recommendation.

Recommendation No. 3: The HCJP recommends: (i) firstly, that the merger should make it possible to bring together, in a single body of rules set out in a single text, the entire regime common to electronic money and payment services (law on payment transactions and payment service contracts); and (ii) secondly, that a single category of payment service providers should be created (the "payment and electronic money institutions" or "**PEMI**") subject to common prudential provisions, customer protection provisions, etc., subject to a few exceptions (minimum capital, redemption of electronic money, etc.).

PSD3/RSP Package: the Commission's proposal is in line with this recommendation because it merges PSD2 and EMD2, creating a single status for payment and electronic money institutions, while preserving certain specificities relating to authorisation conditions, in particular in terms of initial capital and own funds, as well as certain fundamental concepts governing electronic money activities, such as

the issuance of electronic money, the distribution of electronic money and its redeemability.[28]

Recommendation No. 4: The HCJP recommends that a clarification be made between the open universal payment model and the payment system exclusively between affiliates. Without such clarification, there is a risk of persistent confusion between payment services and electronic money or the potential emergence of practical challenges (*e.g.*, reimbursement) that may become insurmountable.

PSD3/RSP Package: the Commission's proposal does not contain any provisions reflecting this recommendation.

Recommendation No. 5: The HCJP recommends that the future text contain a definition of the electronic money medium, for at least two reasons: (i) electronic money is often confused with the underlying device (payment card, payment account) which stores it, thereby hindering its identification and qualification; and (ii) forward-looking, a definition of the electronic money device suitable for covering the future the future *e-money* tokens of the MiCA Regulation.

PSD3/RSP Package: the Commission's proposal does not contain any provisions reflecting this recommendation.

Territorial scope of the PSD

Recommendation No. 6: The HCJP recommends adopting the client solicitation in the European Union as a territorial nexus criterion for the revision of PSD2.

PSD3/RSP Package: the Commission's proposal does not contain any provisions reflecting this recommendation.

Material scope of the PSD - Collection of funds on behalf of third parties

Recommendation No. 7: The HCJP recommends: (i) to clarify the fact that the activity of collecting funds on behalf of third parties involves the provision of identified payment services, so that the qualification is clear to the actors; and (ii) give the EBA the power to draw up regulatory technical standards in order to define the conditions under which the identified services apply.

[28] Proposal for a PSR Regulation, recital 5.

PSD3/RSP Package: the Commission's proposal does not contain any provisions reflecting this recommendation.

Recommendation No. 8: The HCJP recommends indicating that Member States may provide for exceptions concerning identified professions or activities.

PSD3/RSP Package: the Commission's proposal does not contain any provisions reflecting this recommendation.

Exclusions from the scope of the PSD - Technical service providers ("TSP")

Recommendation No. 9: The HCJP recommends clarifying the concepts of "initiation of a payment transaction" and "payment instrument", with a view to specifying the conditions under which: (i) in the case of card payments; and (ii) more generally, the technological solutions provided by technical service providers can be distinguished from the payment services provided by PSPs.

PSD3/PSR package: the Commission's proposal is partly in line with this recommendation: (i) by including a new definition of "initiation of a payment transaction";[29] (ii) by specifying that "*pass-through wallets*", involving the tokenisation of a payment instrument such as a payment card, should be considered as technical services and excluded from the definition of payment instrument and considered as a payment application within the meaning of the Interchange Regulation. However, certain other categories of digital wallets such as prepaid wallets where users can store money for future online transactions should be considered as a payment instrument within the meaning of the PSR;[30] and (iii) providing that it is necessary that, in the future review of this Directive, the Commission pays particular attention to technological developments and assesses whether the scope of the Directive should be extended to cover new services and new risks.[31]

29 "'*initiation of a payment transaction' means the steps necessary to prepare the execution of a payment transaction, including the placement of a payment order and the completion of the authentication process*;" (Article 3(6) of the Proposed PSR Regulation).

30 Recital 24 of the Proposal for a PSR Regulation.

31 Recital 68 *in fine* of the Proposed PSD3.

Recommendation No. 10: The HCJP recommends clarifying the regulatory framework applicable to subcontracting to TSPs, particularly between DORA and the PSD.

PSD3/RSP package: the Commission's proposal is in line with this recommendation.[32]

Recommendation No. 11: The HCJP recommends clarifying the definition of payment system or scheme, so as to link the corresponding exclusion to the submission of the payment system or scheme to the Union's Eurosystem oversight framework for electronic payment instruments, schemes and arrangements ("**PISA**").

PSD3/RSP package: the Commission proposal does not contain any provisions reflecting this recommendation. However, in a recital, it excludes payment systems, schemes or devices from the scope of the text, stating that it wishes to avoid any duplication, particularly with the PISA framework.[33]

Exclusions from the scope of the PSD - Intra-group exclusion

Recommendation No. 12: The HCJP recommends amending the PSD2 to specify in the text of the Intragroup Exclusion that this exclusion applies to the centralisation of payments received from third parties as well as to the benefit of third parties, on behalf of entities belonging to the same group.

PSD3/RSP package: the Commission's proposal is partly in line with this recommendation, as it does not cover the collection of funds received from a third party and owed to a group company.[34]

Payment account

Recommendation No. 13: The HCJP recommends retaining only one definition of payment account, which would be contained in the PSD, with the other relevant texts (in particular, the PAD Directive, the SEPA Regulation and the Interchange Regulation) having to refer to it.

32 Article 81 of the Proposed PSR Regulation.

33 Recital 68 of the Proposed PSD3.

34 Article 2.2(m) of the Proposed PSR Regulation.

PSD3/RSP package: the Commission's proposal does not contain any provisions reflecting this recommendation.

Recommendation No. 14: The HCJP recommends:

- amending PSD2 (either in the recitals or in the definition of payment account) to specify that an account from which payment transactions cannot be made directly but require the use of an intermediary account is not a payment account; and
- that the European legislator and the EBA assess in greater depth whether the concept of third party is relevant to the definition of payment accounts, and to take an explicit position in the interest of legal certainty.

PSD3/RSP package: the Commission's proposal goes further than the recommendation by including an express reference to payments received from and to third parties.[35]

PSP liability

Recommendation No. 15:

- The HCJP recommends that Article 97 of PSD2 be supplemented by a sixth paragraph: (i) allowing account servicing payment service providers (ASPSP) and payment initiation service providers (PISPs) to be able to agree that the strong authentication procedure will be the responsibility not of the ASPSP but of the PISP; (ii) specifying that, in this context, the PISP is liable to the user under the terms of Article 73(1) of the PSD2; and (iii) that the PISP must inform the user beforehand in accordance with Article 52 of the PSD2.
- Consequently, article 73(2) of the PSD2 will also have to be supplemented by a third paragraph providing in substance that it is the PISP that bears the obligation to reimburse the payer for the amount of the unauthorised payment transaction.

[35] Article 2(13) of the Proposed PSD3 and Article 3(15) of the Proposed PSR Regulation: "'*payment account' means an account held by a payment service provider in the name of one or more payment service users which is used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties*;". See also Recital 20 of the Proposed PSR Regulation.

PSD3/RSP package: the Commission's proposal does not contain any provisions reflecting this recommendation. However, the proposal adds new provisions on strong authentication in the context of payment initiation, providing that strong authentication also applies where payments are initiated by an PISP and that the ASPSP must authorise PISPs to rely on its strong authentication procedures.[36]

Recommendation No. 16: The HCJP recommends amending Article 73 of PSD2 to extend the period for reimbursement in the event of an unauthorised payment transaction to five (if the payment service user is a consumer) or fifteen (otherwise) working days instead of one working day as is currently the case.

PSD3/RSP package: the RSP Proposal does not envisage amending the article in this sense.[37]

Recommendation No. 17 : The HCJP recommends amending Article 72 of PSD2 to provide that, where a payment service user denies authorising a payment transaction that has been executed or claims that the payment transaction has not been executed correctly, the PSP may provide evidence "that it did not detect a technical or other deficiency in relation to the service provided which could have affected the transaction", rather than evidence "*that the transaction in question was not affected by a technical or other deficiency in the service provided by the PSP*".

PSD3/RSP package: the RSP Proposal does not envisage amending the article in this sense.[38]

Recommendation No. 18: The HCJP recommends that a new paragraph (3) be added to Article 26 of the PSD2 to allow, but not require, the exchange of information between PSPs for the sole purpose of combating fraud and without professional secrecy constituting an obstacle or being enforceable.

PSD3/RSP package: the Commission's proposal is partly in line with this recommendation, in that it provides for: (i) the possibility of exchanging information between PSPs for the purposes of combating fraud;[39] and (ii) an obligation on telecommunications operators to cooperate with PSPs.[40] In return, PSPs are subject to an obligation to

36 Article 86 of the Proposed PSR Regulation.

37 See Article 56(1) of the Proposed PSR Regulation, unchanged on this point.

38 See Article 55(1) of the Proposed PSR Regulation, unchanged on this point.

39 Article 83(3) of the Proposed PSR Regulation.

40 Article 58(5) of the Proposed PSR Regulation.

monitor payment transactions (*transaction monitoring*) under Article 83(1) of the Proposed PSR Regulation.

Data access

Recommendation No. 19: The HCJP recommends the deletion of Article 94(2) of PSD2 (which provides that PSPs shall only have access to personal data necessary for the performance of their payment services with the explicit consent of the payment service user), as it is not justified in the light of the provisions of the GDPR.

PSD3/RSP package: the Commission's proposal is in line with this recommendation in that it has rewritten the article by referring to the provisions of the GDPR.[41]

Recommendation No. 20: The HCJP recommends replacing the concept of "sensitive payment data" defined in Article 4(32) of PSD2 with that of "protected payment data" and having the following definition: "*data, including personalised security data, which are likely to be used to commit fraud and which require an appropriate level of protection*".

PSD3/RSP package: the Commission's proposal does not propose to change the defined term, but does change the substance of the definition.[42]

Recommendation No. 21: The HCJP recommends:

- concerning strong customer authentication ("**SCA**") and digital identity wallets ("**DIW**"): considering that the ASPSP cannot be responsible for a technical identification and SCA solution over which it has no control and which is imposed on it by the regulations, the revision of PSD2 could provide that in the event of the use of a third-party solution such as the DIW, the user's consent to the execution of payment transactions cannot be contested by the latter with the ASPSP. At best, in the event of a dispute, the ASPSP may only be required to provide assistance in recovering the funds from the beneficiary's PSP;

41 Article 80 of the Proposed PSR Regulation.

42 Article 3(38) of the Proposed PSR Regulation: "'*sensitive payment data' means data which can be used to carry out fraud, including personalised security credentials*;".

- the requirement for dynamic strong authentication required by PSD2 at the initiation of the payment transaction will have to be compatible with the authentication solution proposed by DIW and imposed on ASPSP; and

- with regard to the relationship between the respective revisions of PSD2 and the eIDAS Regulation, given the impact of the draft revision of the eIDAS Regulation on payments, it seems essential to ensure consistency between the revision of this text and that of PSD2. Consequently, it should be recommended that the revision of PSD2, which will have to take account of the revision of the eIDAS Regulation, should only take place once the revision of the eIDAS Regulation has been fully stabilised.

  PSD3/PSR package: the Proposed PSR Regulation does not contain any changes in this respect, but does provide that the PSP retains responsibility for implementing the SCA when this is outsourced to a technical service provider.[43]

[43] Article 87 of the Proposed PSR Regulation.

1. REPLACING THE DIRECTIVE WITH A REGULATION

1.1. Issues related to the question

The revision of PSD2 first involves considering the choice of legal instrument under European Union law. Three options are available:

(a) the first is to replace PSD2 in its entirety by a new directive;

(b) the second is to replace PSD2 in its entirety by a regulation, as was done for the MAR Regulation which repealed and replaced the "Market Abuse" Directive[44] or the Prospectus Regulation which repealed and replaced the Directive of the same name;[45] and

(c) the third option would be to adopt two complementary acts, a directive on the one hand and a regulation on the other hand, following the example of the CRD/CRR package for the banking sector.[46]

The choice depends on the desired degree of uniformity as regards the law applicable to payment services provided in Member States. It is therefore a question of assessing the extent to which divergent national requirements may continue to exist or the degree to which the same rules are to be applied in all Member States.

Based on the multi-jurisdictional analyses contained in this report as well as in the abovementioned EBA and DG FISMA documents, it is possible to identify a number of PSD2 provisions which, as the law currently stands, give rise to differences in application and interpretation between Member States. Examples include:

(i) the concept of a payment account and how it compares with other types of accounts, such as technical accounts;

(ii) the definition of payment institutions' own funds, particularly as regards the calculation of payment volumes (the question of whether only payment

---

44 Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (MAR Regulation), available here.

45 Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, available here.

46 Consisting of Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, available here and Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms, available here.

inflows or outflows, or the total of both, are taken into account in the calculation – one-leg or two-leg payments) gives rise to divergent interpretations, explaining, for example, the differing regulatory practices in Germany and France;

(iii) certain exclusions, such as those of commercial agents or intra-group payment transactions;

(iv) for reserves (the so-called "account footing" technique), there is a difference in interpretation of the requirement to supervise or not supervise the provision of funds collected by a payment service. While some regulators allow the funds to be reserved for future transactions on the accounts of customers acting in a professional capacity (chargeback/refund, in particular), others prohibit it.

In any event, legal certainty, a general principle of European Union law, must be guaranteed.

1.2. **What is the current legal framework?**

The PSD2 is a directive within the meaning of Article 288(3) TFEU. This article provides that *"[t]he Directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods*".

During the preparatory work for PSD2, the choice of legal instrument was not discussed. However, the Commission proposed, without justification, that it should be a "full harmonisation" directive.

Article 107 of the PSD2 is entitled "full harmonisation". It states:

> "*1. Without prejudice to Article 2, Article 8(3), Article 32, Article 38(2), Article 42(2), Article 55(6), Article 57(3), Article 58(3), Article 61(2) and (3), Article 62(5), Article 63(2) and (3), the second subparagraph of Article 74(1) and Article 86, insofar as* ***this Directive contains harmonised provisions, Member States shall not maintain or introduce provisions other than those laid down in this Directive***".[47]

The legislator has chosen, however, not to adopt full harmonisation for the certain provisions (see Appendix IV).

[47] Emphasis added.

The concept of full harmonisation has been clarified by case law. The CJEU has specified that a directive may, on the matters regulated by it, seek to achieve "full harmonisation" of the laws, regulations and administrative provisions of the Member States, without however being intended to "exhaustively" harmonise the field covered by the directive, beyond those matters.[48] Full harmonisation thus relates to "*the latitude allowed to the Member States, and thus to the degree of discretion available to them in transposing the points contemplated by Directive* (…), *while the expression 'exhaustive harmonisation' concerns the scope* ratione materiae *of that directive*".[49]

Where harmonisation is full, Member States have no latitude as regards the transposition of the provisions of the directive: they may not introduce provisions that differ from those contained in those articles. Thus, according to Article 107 of PSD2, "*insofar as this Directive contains harmonised provisions, Member States shall not maintain or introduce provisions other than those laid down in this Directive*".

Harmonisation is not exhaustive, however, in that it is limited to the provisions of the directive, "*with the Member States remaining free to legislate outside those fields, provided that they do not undermine the useful effect of the directive*".[50] Full harmonisation means that Member States must transpose the rules without adding or removing conditions or effects.[51]

Consequently, PSD2 does not intend, in principle, to take away regulatory powers from Member States in the area of payments. Member States may still legislate or regulate matters relating to payments that are not covered by a provision of the directive. However, they do not, in principle, have any latitude as regards the transposition of its provisions.

In theory, full harmonisation reduces the legislative autonomy of the Member States. On the one hand, when the Member State transposes the directive, it must ensure that it complies with its provisions, which may nevertheless cover imprecise or ambiguous concepts. On the other hand, outside the transposition process, Member States must also enact their rules in compliance with the provisions of the directive. As a result, full harmonisation is of such normative intensity that it

---

48 CJEU,4 June 2009, *Moteurs Leroy Somer*, C-285/08, EU:C:2009:351, point 25, available here..

49 *Opinion of advocate general, delivered on 8 July 2021, C-337/20, DM & LR v. Caisse régionale de Crédit agricole mutuel (CRCAM) – Alpes-Provence*, point 69, available here.

50 *Ibid*, point 70.

51 J. ROCHFELD, "*Les ambiguïtés des directives d'harmonisation totale : la nouvelle répartition des compétences communautaire et interne*", *Dalloz actualité* 14 September 2009, § 4, available here.

"*imposes rules which entirely replace existing national rules on the subject*".[52] This means that Member States no longer have the option of adopting national rules for matters governed by the provisions of the directive.[53] However, this substitution is purely substantial in that the Member States are formally obliged to adopt transposition measures that incorporate the provisions of the directive. The fact remains that national authorities and institutions apply rules laid down by provisions of national law.

While it differs from exhaustive harmonisation, full harmonisation is more similar to complete harmonisation. It also depends on the normative input of the provisions of the directive. In fact, full harmonisation refers to directives' provisions whose content proves to be sufficiently complete that they do not call for any additional substantial intervention by the Member State. The provision of a complete or total harmonisation directive exhausts the competence of the Member State in that it cannot add any further requirements.

As a result, full harmonisation directives are similar to regulations. Article 288(2) of the TFEU provides that regulations shall have general application, shall be binding in their entirety and shall be directly applicable in all Member States. The provisions of regulations do not, in principle, require any measures of incorporation into the national legal order. However, there is an essential difference between a regulation and a complete harmonisation directive. The provisions of directives must, in any case, be transposed into national law, in accordance with Article 288(3) of the TFEU. Although transposition generally takes the form of a legislative or regulatory provision, it is not necessary where national law is already compatible with the provisions of the directive. However, even in case of full harmonisation, Member States adopt transposition measures which formally incorporate the substantive content of the directive into national law. The Member State may thus opt to merely copy the requirements set out in the provisions of the directive. However, in practice, there may still be differences in national transposition, either because the provisions of the directive may be imprecise and lead to interpretations that differ from one Member State to another, or because the concepts used are generally complex and do not always cover legal concepts that exist in the national legal systems. Intrinsically, even a full harmonisation directive may therefore present a risk of normative divergences as regards its transposition and application in the Member States. Conversely, a regulation guarantees uniform application in all Member States.

---

52 A. MATTERA, *Le marché unique européen*, Jupiter, 1990, 2e ed., p. 180.

53 ECJ, 25 April 2002, *Commission v/ French Republic*, C-52/00, ECLI:EU:C:2002:252, available here; ECJ, 25 April 2002, *Commission v/ Greece*, C-154/00, ECLI:EU:C:2002:254, available here.

1.3. **Available options**

1.3.1 *The legal basis*

It should be noted at the outset that Article 114 of the TFEU is the legal basis for the PSD2.

The EU legislator may adopt both regulations and directives on the basis of this provision. It also has the right to replace a directive with a regulation. There are precedents for this, such as the Market Abuse Regulation, which repealed Directive 2003/6/EC of the European Parliament and of the Council and three other directives of the Commission[54] , as well as the Prospectus Regulation, which repealed and replaced the directive of the same name.[55]

The choice between a regulation and a directive is a political decision to be made by the Commission in the exercise of its power of initiative and by the European Parliament and the Council in the exercise of their legislative function. In the spirit of the Treaty, the difference between regulations and directives is explained by two visions of the normative relationships in the legal order of the European Union.

1.3.2 *Regulations and directives*

As anticipated, under Article 288 of the TFEU, regulations and directives do not have the same characteristics.

Once it has entered into force, the regulation produces full legal effects without the need for any reception measures. It is therefore directly and immediately applicable in the legal order of the Member States both in vertical relations, *i.e.*, between the State *lato sensu* - the national authorities - and individuals, and in horizontal relations, *i.e.*, between individuals. This means that the provisions of a regulation can be invoked and applied both in relations between public authorities and institutions and in relations between individuals (institutions between themselves or with customers). The regulation implies the harmonisation of law in national legal systems: it applies by itself in all Member States. Thus, to justify the MAR "market abuse" regulation's replacement of the directive, the legislator indicated the need to "*ensure that there are uniform rules and clarity of key concepts*".[56]

---

54 Regulation (EU) No 596/2014 cited above.

55 Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market.

56 Recital 3 Regulation (EU) No 596/2014.

In contrast, the directive requires national transposition measures. Article 288(3) of the TFEU places an obligation on the Member State to bring its legal system into line with the objectives of the directive. The directive provides for a transposition period - ranging from several months to several years - by the end of which national measures must have been adopted. During this period, the Member State must refrain from taking any measures that could seriously compromise the achievement of the result prescribed by the directive. On expiry of the transposition deadline, national law must be compatible with the objectives of the directive. If such is not the case, the provisions of the directive may be invoked by individuals, provided that they are clear, precise and unconditional, but only in vertical ascending relations; in other words, an individual may invoke the said provisions of the directive against national authorities alone. An individual cannot however invoke the directive directly against another individual. In any case, national law must always be interpreted in accordance with the directive. It can therefore be invoked in all vertical and horizontal relations for the purposes of consistent interpretation.

The distinction between a regulation and a directive is therefore crucial in two regards.

In terms of timing, while the entry into force of a regulation is immediate, a directive only produces its full effects in the national legal order, through national law, when the deadline for its transposition has expired. This means that a period, during which divergences between national laws persist, remains between the date of entry into force of a directive and the date of expiry of the transposition period.

From a normative point of view, a regulation produces its own effects in the national legal order, which leads to a harmonisation of the substantive rules in the field it governs. Its provisions apply in all Member States. In contrast, a directive does not apply by itself even if it is a complete harmonisation directive. If it has been correctly transposed, the provisions of national law are applied, which leads to the formal coexistence of 27 national laws which, in theory only, converge in their substance. A divergence in national laws is thus maintained since the national transposition provisions apply in each Member State and are interpreted where necessary in accordance with the directive which is intended solely to enable the approximation of national legislative and regulatory provisions. Admittedly, the directive is of interest when the national provisions in question fall within areas of national competence. This is the case when concepts of civil law or commercial law, which are typically national, need to be addressed. However, the competence argument is by no means decisive. While the EU does not have general competence to harmonise civil or commercial law of Member States, article 114 of the TFEU is the appropriate legal basis for harmonising those national provisions that are likely to impede the free movement of services and payments.

1.3.3 *The choice of regulation*

The working group concluded that the directive should be replaced by a regulation. A regulation is far more appropriate as to have uniform rules in all Member States, whereas a directive carries the risk of persistent national divergences.

In any event, it is hardly appropriate to replace the directive with two instruments, a regulation and a directive. As it is the case in banking area, with the articulation between the CRD and the CRR, the coexistence of a regulation and a directive makes the regulatory framework more complex because of cross-references not only between the regulation and the directive, but also between national transposition measures and the regulation.

The choice of a regulation is explained by the need to guarantee legal certainty, which is a general principle of EU law that must be respected by the European legislator.

There are two sets of considerations that justify recourse to a regulation. Recital 5 of the MAR Regulation is enlightening, in this respect, as it clarifies the arguments that justified the replacement of the directive by the regulation.[57]

From an economic point of view, the regulation promotes uniformity of rules to avoid the risk of fragmentation of the internal market for payment services. The transposition of the directive leaves open the risk of divergent regimes being applied in different Member States. This leads to maintaining of the distortions of competition which are sharpened by the forum shopping that Member States could engage in by exploiting the options and imprecisions contained in the directive. The divergence of national legal frameworks may indeed constitute a factor of competitiveness and attractiveness that certain Member States seek by exploiting the latitudes left by the directive.

From a legal point of view, the uniformity promoted by the regulation makes it possible to foster the free movement of payment operators who intend to carry on

---

[57] *"In order to remove the remaining obstacles to trade and the* ***significant distortions of competition resulting from divergences between national laws*** *and to prevent any further obstacles to trade and significant distortions of competition from arising, it is necessary to adopt* ***a Regulation establishing a more uniform interpretation of the Union market abuse framework****, which more clearly defines rules applicable in all Member States. Shaping market abuse requirements in the form of a regulation will ensure that those requirements are directly applicable. This should ensure* ***uniform conditions by preventing diverging national requirements as a result of the transposition of a directive****. This Regulation will require that all persons follow the same rules in all the Union. It will also reduce regulatory complexity and firms' compliance costs, especially for firms operating on a cross-border basis, and it will contribute to eliminating distortions of competition"*. Emphasis added. Recital 5 of Regulation (EU) No 596/2014, cited above.

their business on a cross-border basis. With uniform provisions, operators would not have to bear the costs of complying with each national law, costs that can have a significant dissuasive effect, thereby hindering freedom of movement.

However, one member of the sub-group drew attention to the major work involved in transposing the first payment services directive into the Financial Code [58] [59] . The transformation of the directive into a regulation should necessarily lead to an "unravelling" of the provisions of the directive incorporated in a coherent manner into our legislative corpus, which we could regret, given the quality of the transposition at the time that goes beyond the purely "literal".

1.3.4 *Referral to level 2 measures*

In the choice between regulation and directive, between uniformity of law and harmonisation of national laws, one argument in favour of the directive could be the reference to level 2 measures. In essence, the future directive would leave the tasks of establishing uniform provisions where appropriate throughout the Union to delegated acts under Article 290 of the TFEU or implementing acts under Article 291 TFEU. A directive may in fact instruct the Commission to adopt delegated or implementing regulations which have the advantage of standardising the law where this subsequently proves necessary.

However, referring to level 2 measures is far from a panacea.

First, in terms of timing, a period of 18 to 24 months occasionally can elapse between the entry into force of the legislative act and the adoption of the delegated or implementing act. This is likely to fuel legal uncertainty, especially as the adoption of implementing acts involves recourse to comitology, which can make the applicable law unnecessarily complex.

Second, the choice of whether to refer to a delegated act or an implementing act must take account of the desire to involve the European supervisory authorities (in particular, the EBA) in drawing up the regulations.

---

58 See Ordinance 2009-866 of 15 July 2009 on the conditions governing the provision of payment services and the creation of payment institutions, transposing Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

59 Revue Banque - hors-série décembre 2009 - La pratique du droit bancaire - Transposition de la directive 2007/64/CE sur les services de paiement - Les nouvelles règles régissant la relation banque-client - Emmanuel JOUFFIN, Olivia LAPLAGNE, Catherine L'HOSTIS

1.3.5 *Penalties*

In choosing between a regulation and a directive, the question of penalties also arises. As the law currently stands, Article 103 of the PSD2 provides that: "*Member States shall lay down rules on penalties applicable to infringements of the national law transposing this Directive and shall take all necessary measures to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive*".

The solution is a classic one. To ensure the effectiveness of the directive, the power to impose penalties is exercised by the national authorities in accordance with the principle of institutional and procedural autonomy. It is up to each Member State to designate the authority or court competent to sanction breaches of the rules arising from the directive (or regulation).

If, however, the europeanisation of penalties is envisaged, a regulation would be necessary. This would involve empowering an EU institution - for example the Commission or the ECB - or an EU body - for example a European supervisory authority - to exercise a power of imposing penalities directly against individuals. On the basis of Article 114 of the TFEU, it is possible to enshrine a power of imposing sanctions. However, this requires the adoption of a regulation which, moreover, must lay down precisely the conditions for exercising such a power.

1.4. **HCJP recommendations**

The working group considers that a regulation is likely to guarantee uniform application of the rules relating to payment services and that the precedent constituted by the CRD/CRR package can be weighed against the Benchmark and MiCA regulations which govern both access to the profession by the national authorities of Member States and their supervision by these authorities as well as the provision of regulated services in accordance with uniform rules which are directly imposed in the legislation of the Member States. Such uniformity is required to guarantee the free movement of payment services and therefore to promote the completion of the internal market for these services.

> **Recommendation No. 1:** The HCJP recommends that the Directive be replaced by a Regulation.

2. MERGER OF PSD2 AND EMD2

The question of merging PSD2 and EMD2 raises another issue: that of the autonomy of electronic money, its concept, its regime and, more broadly, its regulation, in relation to the category of payment services and the law built up by PSD1 and PSD2.

However, the question of a merger between payment services and electronic money is not new. It arose during the revision of EMD1.[60] As for EMD2, the evaluation report that was due by 1 November 2012, and was finally delivered on 25 January 2018, stressed that "*one of the key challenges identified by the economic study is the classification of products and services as e-money or as payment services, as e-money accounts or payment accounts, and thus the application of the appropriate legal framework*". [61]

2.1. Issues related to the question

First, it's important to recall the legal definitions of electronic money:

Text	Provisions concerned	Layout
EMD2	Article 2(2)	*"electronic money" means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer*
Financial Code	Article L. 315-1	*I. - Electronic money is monetary value stored in electronic form, including magnetic form, representing a claim on the issuer, which is issued against the delivery of funds for the purposes of payment transactions as defined in Article L. 133-3 and which is accepted by a natural or legal person other than the electronic money issuer.*

60 *"From a purely legislative perspective, the ideal objective should be to incorporate the E-money Directive into the Payment Services Directive*", Commission staff working document on the review of the e-money directive (2000/46/EC), 19 July 2006, SEC(2006) 1049, p. 15.

61 European Commission, "Report from the Commission to the European Parliament and the Council on the implementation and impact of Directive 2009/110/EC, in particular one the application of prudential requirements to electronic money institutions", COM(2018) 41 final, 25 Jan. 2018, p. 9.

		II. - Units of electronic money are referred to as units of value, each of which constitutes a claim embedded in a security.

We should also recall an old definition given by the ECB, which is still very relevant: "*Electronic money is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction but acting as a prepaid bearer instrument*".[62]

As for PSD2, the explanatory memorandum to the proposed PSD2 states: "*At a time when the distinction between payment institutions (subject to the PSD) and electronic money institutions (subject to Directive 2009/110/EC of the European Parliament and of the Council2 , the second Electronic Money Directive or 'EMD') is increasingly blurred as technology and business models converge, a full modernisation of the digital payment framework resulting in the merger of both categories of actors and respective legislations would be optimal.*"[63] The idea is taken up in the Commission's 2020 communication on a retail payments strategy for the EU. [64]

In other words, is the issuing and management of electronic money a payment service like any other? The abovementioned Commission communication would suggest so: "*(...) as part of the PSD2 review, [it will] align the PSD2 and E-Money Directive (EMD2) frameworks by including the issuance of e-money as a payment service in PSD2*".[65]

But this would more or less lead to the denial of the autonomy of electronic money, at the risk of rendering it useless.

---

62 ECB, "*Report on electronic money*", August 1998, p. 7, available here.

63 Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, COM(2013) 547 final, 24 July 2013, p. 3, available here.

64 *"While PSD2 implementation is still in its infancy, the E-money Directive (EMD2)48 has been in force for over a decade, so there is sufficient experience to draw lessons from its implementation. After the adoption of PSD2, the two regimes converged, but remained separate. The differences between the services provided by payment institutions and e-money institutions no longer seem to justify a distinct authorisation and supervision regime and could therefore be brought under a single framework.*", COM(2020) 592 final, 24 Sept. 2020, p. 21.

65 COM(2020) 592 final, p. 23.

2.2. What is the current legal regime?

Today, two texts coexist, but their coexistence is marked by a time lag: EMD1 dates from 2000[66], while PSD1 was adopted in 2007.[67] Consequently, EMD2[68] logically preceded PSD2[69] .

In addition to this time lag, there are multiple cross-references between EMD2 and PSD1 (before PSD2), which does not make the electronic money regime any easier to understand. This is undoubtedly a source of confusion.

2.2.1 *Electronic money in EMD2*

As its title indicates, EMD2 does not relate directly to electronic money (as PSD2 does with payment services), but concerns the taking up, pursuit and supervision of the activity of electronic money institutions (EMIs) (following the example of the CRD). This is an argument in favour of an "electronic money" object that would not directly be comparable to a "service" but would characterise, upstream, a "means of payment", or even a "*genuine payment system", made up of an issuer, cardholders/user and a network of merchants*".[70]

(a) The recitals of the EMD2

Clearly, EMD2 does not stand on its own, and recital 3 refers to what was then PSD1, which "*established a modern and coherent legal framework for payment services*".

This dependence of e-money law on payment services law is perfectly illustrated in recital 9 of the EMD2.[71]

---

66 Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

67 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.

68 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

69 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.

70 S. Lanskoy, "The legal nature of electronic money", Bulletin Banque de France No. 70, Oct. 1999.

71 "*The prudential supervisory regime for electronic money institutions should be reviewed and aligned more closely with the risks faced by those institutions. That regime should also be made coherent with the prudential supervisory regime applying to payment institutions under Directive 2007/64/EC. In this respect, the relevant provisions of Directive 2007/64/EC should*

It is further specified in recital 19 (and repeated in Article 13 of EMD2) that "*chapter 5 of Title IV of Directive 2007/64/EC should therefore apply mutatis mutandis in the context of this Directive, without prejudice to the provisions of this Directive. A reference to 'payment service provider' in Directive 2007/64/EC therefore needs to be read as a reference to electronic money issuer; a reference to 'payment service user' needs to be read as a reference to electronic money holder; and a reference to Titles III and IV of Directive 2007/64/EC needs to be read as a reference to Title III of this Directive*", and "*a reference to Titles III and IV of Directive 2007/64/EC needs to be read as a reference to Title III of this Directive*".

Finally, recital 24 of EMD2 states that "*this Directive introduces a new definition of electronic money, the issuance of which can benefit from the derogations in Articles 34 and 53 of Directive 2007/64/EC*".

(b) **The provisions of the EMD2**

The dependence of the electronic money regime on payment services law is clear from Article 1 of EMD2 as regards its purpose and scope, insofar as paragraphs (4) and (5) exclude from it the monetary value, which is itself left out under Article 3(k) and (l) of PSD1.

The definition of electronic money also refers to the PSD1:

> "'*electronic money' means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer*"[72].

---

apply mutatis mutandis to electronic money institutions without prejudice to the provisions of this Directive. A reference to 'payment institution' in Directive 2007/64/EC therefore needs to be read as a reference to electronic money institution; a reference to 'payment service' needs to be read as a reference to the activity of payment services and issuing electronic money; a reference to 'payment service user' needs to be read as a reference to payment service user and electronic money holder; a reference to 'this Directive' needs to be read as a reference to both Directive 2007/64/EC and this Directive; a reference to Title II of Directive 2007/64/EC needs to be read as a reference to Title II of Directive 2007/64/EC and Title II of this Directive; a reference to Article 6 of Directive 2007/64/EC needs to be read as a reference to Article 4 of this Directive; a reference to Article 7(1) of Directive 2007/64/EC needs to be read as a reference to Article 5(1) of this Directive; a reference to Article 7(2) of Directive 2007/64/EC needs to be read as a reference to Article 5(6) of this Directive; a reference to Article 8 of Directive 2007/64/EC needs to be read as a reference to Article 5(2) to (5) of this Directive; a reference to Article 9 of Directive 2007/64/EC needs to be read as a reference to Article 7 of this Directive; a reference to Article 16(1) of Directive 2007/64/EC needs to be read as a reference to Article 6(1)(c) to (e) of this Directive; and a reference to Article 26 of Directive 2007/64/EC needs to be read as a reference to Article 9 of this Directive.".

[72] Article 2(2) of the EMD2.

The prudential regime for EMIs still borrows heavily from that of PIs[73] , as does the calculation of own funds for activities not related to the issuance of electronic money (this issue is at the heart of the Paysera ruling, discussed below)[74].

With regard specifically to the activities of EMIs, Article 6 of EMD2 empowers them to provide payment (and ancillary services) within the meaning of PSD1, as well as obliges them to safeguard funds received in exchange for electronic money issued in accordance with Article 9(1) and (2) of PSD1[75].

Finally, as regards optional exemptions, EMD2 and PSD1 seem to form a single text:

> "*Member States may waive or allow their competent authorities to waive the application of all or part of the procedures and conditions set out in Articles 3, 4, 5 and 7 of this Directive, with the exception of Articles 20, 22, 23 and 24 of Directive 2007/64/EC, and allow legal persons to be entered in the register for electronic money institutions if both of the following requirements are complied with (...)*"[76]

2.2.2 *Electronic money in PSD2*

Conversely, the PSD2 (which, incidentally, has modified the EMD2 in a number of aspects)[77] has on several occasions asserted its hold on electronic money, over and above its own prudential regime.

Recital 25 of the PSD2 is a case in point:

> "*This Directive lays down rules on the execution of payment transactions where the funds are electronic money as defined in Directive 2009/110/EC. This Directive does not, however, regulate the issuance of electronic money as provided for in Directive 2009/110/EC. Therefore, payment institutions should not be allowed to issue electronic money*."

This is because the "funds" involved in payment transactions can just as easily, and indiscriminately, consist of "*banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC*"[78] (not to be

---

73 Article 3(1), (4) and (5) of the EMD2.

74 Article 5(2) of the EMD2.

75 Article 7(1) of the EMD2.

76 Article 9(1) of the EMD2.

77 Article 111 of the PSD2.

78 Article 4(25) of the PSD2.

confused with funds received by PIs from payment service users, which are neither deposits nor electronic money)[79].

Articles 42 and 63 of the PSD2 also lay down common rules for low-value payment instruments and electronic money.

2.2.3 *Electronic money in French law*

The Financial Code expressly states that the law governing the execution of payment transactions applies to the issuance and management of electronic money[80].

Conversely, article L. 315-5 of the Financial Code makes contract law relating to payment services the standard for electronic money issuing and management activities. [81]

2.2.4 *Other legislation on electronic money*

(a) **Prepaid cards**

Prepaid cards are very generally considered as electronic money payment instruments, most of which are "anonymous", hence the somewhat overused expression "anonymous electronic money"[82].

Prepaid cards, for example, are referred to in the Regulation on interchange fees for card-related payment transactions, where they are defined as "a category of payment instrument on which electronic money, as defined in point 2 of Article 2 of Directive 2009/110/EC, is stored"[83].

They are also mentioned in Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the

---

79 Article 18(3) of the PSD2.

80 See Article L. 133-1-VII of the Financial Code: "*Without prejudice to the application of Section 12* [Terms and conditions of redemption of electronic money]*, this chapter* [Rules applicable to other payment instruments and access to accounts] *shall apply to the issuance and management of electronic money*".

81 Cf. article L. 315-5 of the Financial Code: "*Chapter IV* [Payment services] *of this Title* [Banking, payment services and the issuance and management of electronic money] *shall apply to the business of issuing and managing electronic money, without prejudice to the additional requirements set out in this section*".

82 For example, see Banque de France, "La surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers", 2017 Report, pp. 37 et seq. See also M. Perdrix, "La problématique des paiements par cartes prépayées", Bulletin Banque de France 1994, p. 93.

83 Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-related payment transactions, Article 2(35).

Union and repealing Regulation (EC) No 1889/2005, where, together with currency, bearer-negotiable instruments and commodities used as highly liquid stores of value, they make up the "cash" category:

> "*'prepaid card' means a non-nominal card, as listed in point 2 of Annex I, that stores or provides access to monetary value or funds which can be used for payment transactions, for acquiring goods or services or for the redemption of currency where such card is not linked to a bank account*"[84] (art. 2, f)).

Moreover, their anonymity has necessarily been subject to regulation in terms of the fight against money laundering and combating the financing of terrorism (AML/CFT). This partly justified the revision of the 4th anti-money laundering directive[85] by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 (the anonymity of "virtual currencies" was also targeted).

(b) **Digital exchange media**

Even more anecdotal is the category of "*digital means of exchange*", which Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA defines as follows: "*any electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council or virtual currency*" (Art. 2(c)).

(c) **Crypto-assets**

The European Commission has announced that " *in the proposal for a Regulation on Markets in Crypto Assets, [it will] subject issuers of emoney tokens to additional provisions complementing EMD2*"[86].

Electronic money is omnipresent in the MiCA Regulation. In particular, there is the category (and even the first category of crypto-assets) of *e-money* tokens (EMTs), which are described in Recital 18 of the Regulation as "*(...) crypto-assets that aim to stabilise their value by referencing only one official currency. The function of such crypto-assets is very similar to the function of electronic money as*

---

84 It should be noted that the regulation refers to the concept of "bank account", which is not defined in European payment services law. It should probably read "payment account". See the discussion on this subject in paragraph 7.1.1 below.

85 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) Nº 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

86 COM(2020) 592 final, p. 23.

defined in Directive 2009/110/EC. Like electronic money, such crypto-assets are electronic surrogates for coins and banknotes and are likely to be used for making payments. Those crypto-assets should be defined in this Regulation as 'e-money tokens'".

It is worth noting that *e-money tokens* feature prominently in the DG FISMA study published on 2 February 2023, which suggests in particular that MiCA and PSD2 should be consolidated (see below).

(d) **AML/CFT**

The amended 4th anti-money laundering directive, after defining electronic money by reference to Article 2(2) of the EMD2[87] , provides for a lighter due diligence regime for a very limited use of electronic money[88].

Article 45(9) gives Member States the option of requiring European EMIs (and PEs) established in their territory in a form other than a branch to appoint a central contact point.

As for the regulation accompanying the directive (4th anti-money laundering regulation[89]), it has the advantage of referring several times to transfers of funds "*in cash or in the form of anonymous electronic money*"[90].

2.2.5 *Case law on electronic money*

It is still very rare, but at least two decisions, including the first especially, can be listed.

(a) **"Paysera" ruling**

Reference is made here to the first important ruling on e-money: the *Paysera* judgment, handed down by the CJEU on 16 January 2019[91] .

Not only does it rule on the concept of "*payment services linked to the issuance of electronic money*", in order to resolve a question of calculating own funds that involve EMD2 and PSD1 (in this case), but it also affirms the "redeemability" of

87 4th AML/CFT Directive, Article 3(16). See also Annex II which lists, among the factors and types of items with potentially lower risk, "*products for which the risks of money laundering and terrorist financing are controlled by other factors such as the imposition of loading limits or transparency of ownership (e.g. for certain types of electronic money)*".

88 4th LCB-FT Directive, article 12.

89 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) Noº 1781/2006.

90 4th LCB-FT Regulation, article 5(3), a), article 6(2)(b) and article 7(4)(a).

91 CJEU, 16 Jan 2019, *Paysera LT UAB*, C-389/17, ECLI:EU:C:2019:25, concl. advocate general M. Wathelet.

electronic money: "*(...) the issuance of electronic money unconditionally and automatically confers entitlement to redemption (...)*" (point 28).

Therefore, a future PSD 3 incorporating e-money law should provide for this new dimension of redeemability of e-money, which is a notion typical of the nature and regime of e-money, that its holder can exercise at any time by virtue of its claim on the issuer. It should be noted that this right of claim against the issuer of electronic money is an element which distinguishes scriptural money from electronic money, in that the bank is not the debtor of the money issued by the issuing institution (for the euro, the ECB), but is the debtor of a claim for restitution of the deposit made by the depositor. When electronic money is transferred, the beneficiary who receives the electronic money is therefore transferred a claim against the issuer of the electronic money.

(b) Decision of the Conseil d'état

Mention should also be made of what would be the *Conseil d'Etat*'s first decision on the qualification of electronic money,[92] albeit of very limited scope:

> *"(...) the company, which is licensed as an electronic money institution, offers its customers the possibility of acquiring, by any usual means, from a sales outlet in its network, which is essentially made up of tobacconists, a ticket that includes an electronic PIN code that it issues and to which is associated a line of monetary value that can either be consumed online at merchant sites, in particular online gaming and betting sites, that accept this method of payment, or reimbursed subject to conditions up to the amount of the claim held against the company. It follows that the Ticket Premium product marketed by Wari Pay constitutes electronic money within the meaning of Article L. 315-1 of the French Monetary and Financial Code*"[93] .

[92] See E. Rogey and M. Pachebat, "Le Conseil d'État confirme l'interdiction temporaire d'activité d'un établissement de monnaie électronique pour défaut de protection des fonds des clients", RDBF No. 1, Jan-Feb 2023, Study 4, No. 8.

[93] CE, 9th and 10th ch. Réunies, 9 Dec. 2022, *société WariPay*, no. 4565582, concl. C. Guibe.

2.3. Available options

2.3.1 *Work*

(a) Report from the Commission to the European Parliament and the Council

The abovementioned 2018 Commission report remains very cautious about the prospect of a merger between PSD2 and EMD2 :

> *" A future revision of the Directive and its merger with the revised Payment Services Directive would require further analysis. It seems appropriate to consider such steps only after Member States and stakeholders will have been able to gather experience with the adapted framework following the adoption of PSD2, which will also have an impact on e-money institutions*"[94].

(b) EBA response to the Commission's call for advice[95]

In its response of 23 June 2022, the EBA expresses its full support for the idea of a merger between PSD2 and EMD2 and further proposes:

(i) cover the electronic money services in the existing payment services due to their very similar nature and applicable risks;

(ii) apply identical legal requirements for PIs and EMIs, in particular in relation to the authorisation process and the requirements on safeguarding, initial capital and own funds; and

(iii) clarify the nature and status of distributors of electronic money and apply a coherent framework to agents and distributors.

Incidentally, it should be noted that the EBA[96] curiously states that it has identified two potential ways of achieving unification between payment services and electronic money:

(A) the first would be to consider that all e-money-related services are covered by the existing payment services in Annex I to PSD2, thereby eliminating

---

94 COM(2018) 41 final, 25 Jan. 2018, p. 8.

95 EBA, "*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*", EBA/Op/2022/06, 23 June 2022 .

96 EBA, *op. cit*. nos. 109, 110 and 111.

the need to delineate between scriptural money and electronic money, which can both be encompassed in the term "funds"; and

(B) the second would extend the list of payment services to include only "*hardware-based electronic money services, which are stored on pre-paid cards that are not linked to accounts*".

(c) EBA report on the review of authorisations under PSD2

Published on 11 January 2023, the EBA report calls on the European Commission, "in order to *ensure more consistency and harmonisation across the EU and to create a level playing field*", to "*provide clear criteria in order to delineate between the different categories of payment services as well as e-money issuance*". [97]

(d) DG FISMA study[98]

The study by DG FISMA,[99] dated 2 February 2023, is intended to prepare directly for the revision of PSD2.

Under Pillar 1 (PSD2 scope and exclusions), it is recommended to "*unify PSD2 and EMD2 to address legal uncertainty and diverging application of rules across countries and for different market participants. To address this a legislative consolidation between the two texts is proposed by:*

1. Adding a chapter on the authorisation and supervisory requirements for electronic money institutions in the PSD2 Title on PSPs;

2. Extending the application of Titles III and IV of the PSD2 to e-money payment transactions;

3. Removing preamble (6) of EMD2; and

4. Setting a single set of core definitions applicable both to e-money and payment services.".

The report goes on to recommend "***more consistent definitions of the following main issues: access to accounts (within the PSD2+EMD2), access to payment systems (better within the FSD), agents/outsourcing (within the PSD2+EMD2).*** *There are divergent approaches at national level to the "agent" exemption;*

---

97 EBA/REP/2023/01, paragraph 187.

98 DG FISMA, "*A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*", FISMA/2021/OP/0002 .

99 It is 188 pages long, with 172 pages of appendices.

divergent application practices for direct and indirect access of EMI and Pis to payment systems, which creates legal uncertainty, slows the development of cross-border payments and represents a market barrier. To address this, the following recommendations are proposed:

1. EBA guidelines on the "agent" exemption on a regular basis;

2. EBA guidelines on the indirect access of EMIs and Pis to payment systems; and

*3. Consolidating the guidelines, PSD2 provisions and Q&As on "access to accounts" in the ASPSPs-TPPs relationship".*DG FISMA also proposes to "*strengthen cooperation between national supervisory authorities over payment platforms and digital platforms providing payment services to prevent divergent application of PSD2 and divergent supervisory practices. This will reduce legal uncertainty about PSD2 rules and reduce costs for businesses. To address this, the following recommendations are proposed:*

1. Giving a legal framework to digital platforms providing payment services (for example: Amazon; Apple Pay, and so on) as foreseen in the DMA; and

2. Setting up a supervisory committee on platforms on a cross-border basis coordinated by EBA"[100]

The DG FISMA study also focuses significantly on the subject of electronic money and digital wallets, which leads it to take an interest in "Big Techs", the majority of which, it notes (but without drawing any significant conclusions), have chosen the EMI status, as illustrated by the table below:

[100] DG FISMA, *op. cit.* pp. 17 and 18.

Table 5 BigTech Payment Licence in Europe

BigTech Firm	Year of Licence	Type of Licence	EEA National Competent Authority
PayPal	2007	Banking Licence	CSSF- Luxembourg
Amazon Payments Europe	2010	E-money Licence	CSSF- Luxembourg
eBay	2014	Payment Institutions Licence	CSSF- Luxembourg
Rakuten Europe Bank	2016	Banking Licence	CSSF- Luxembourg
Facebook Payment Intl Ltd	2018	Payment Institutions Licence	Central Bank of Ireland
Alipay Limited	2018	E-money Licence	CSSF- Luxembourg
Airbnb Payment	2018	E-money Licence	FCA-UK
Google Payment Lithuania	2018	E-money Licence	Lietuvos Banka-Lithuania
Google Payment Ireland	2019	E-money Licence	Central Bank of Ireland
Uber Payment	2019	E-money Licence	De Nederlandsche Bank-Netherlands
Takeaway.com	2019	Payment Institutions	De Nederlandsche Bank-Netherlands
Zalando Payment Solution	2019	E-money	BaFin – Germany

On the advisability of merging EMD2 and PSD2, we refer to page 108 of the study (which has the advantage of presenting the arguments against), as well as to pages 113 to 115 devoted to the concept of *'e-money'*. In particular, it states: "*The vast majority of stakeholders consulted noted that since EMIs in effect appear to be providing the same payment services they agree with proposals to merge EMD2 and PSD2 into one text and add e-money as part of the definitions of a payment service."*[101].

2.3.2 *Towards the merger of PSD2 and EMD2*

In all likelihood, we are moving towards a single text: PSD 3 (or its equivalent in the form of a regulation), which would merge payment services law and e-money law.

A consensus is emerging in favour of this merger, if only to clarify a legal framework that has hitherto been considered complex, unclear and impractical.

Nevertheless, it is not yet known whether PSD 3 will carry out a "technical" merger (i.e. incorporate the provisions of EMD2 as they stand) or, on the contrary, take advantage of the opportunity to recompose, in part, payment law, in particular the

101 DG FISMA, *op. cit.* p. 113.

"institutional" aspect with the creation of a single "payment and electronic money institution" with a unified prudential regime.

It is reasonable to think that this announced merger would create an opportunity to correct and enrich the electronic money regime which, incidentally, has undoubtedly became outdated since 2009. In this respect, the digitisation of payments that we are witnessing should not leave the concept or the system of electronic money untouched.

However, such an incorporation of e-money law into payment services law should not be at the expense of a "watering down", or even a "dilution", of the concept and interest of e-money.

(a) **What is desirable**

First of all, it seems desirable to bring together in a single text (PSD 3) the rules that were previously scattered throughout EMD2 and PSD2 and that apply equally to PIs and EMIs (authorisation, prudential provisions, protection of funds, etc.) and to their supervision, the contracts they enter into (contractual information, framework payment services contracts), internal control (including outsourcing), the European passport and AML/CFT obligations.

Similarly, as EMIs are first and foremost PSPs, it would be good legislation if a body of rules common to the provision of payment services by both PIs and EMIs was to be included in the future PSD 3. Moreover, as has already been emphasised, the rules relating to payment transactions (authorisation, execution, dispute) are irrelevant to the status of the PSP. Whether the funds consist of cash, scriptural money or electronic money (and, soon, crypto-assets, when the regulation on information accompanying transfers of funds and certain crypto-assets applies), the same law on the execution of payment transactions should apply.

Finally, we are likely to see a merger between agents (PSPs) and distributors (e-money), whose distinction and difference in regime (registration in one case, simple information to the supervisor in the other) are not or no longer justified.

Generally speaking, a single text would remedy what could appear to be a pointless and prejudicial fragmentation of the rules applicable to payments (in scriptural as well as electronic money).

(b) **What isn't (or would be dangerous)**

On the other hand, it seems to us that it would be detrimental to the autonomy, if not the existence, of electronic money to make it a payment service like any other; for example, to classify the issuance (and management) of electronic money as a 9°

service (as it stands in the Annex to PSD2 and in paragraph II of Article L. 314-1 of the Financial Code).

In fact, we believe that electronic money is upstream of the qualification of payment service, in the sense that it is a genuine "means of payment" (although the concept is little used in European law and is improperly used in the Financial Code), or even a scheme or system of payment in its own right.

That electronic money is more than a payment service is dictated by point 25 of Article 4, which defines "*funds*" as "*banknotes and coins, scriptural money or electronic money defined in point (2) of Article 2 of Directive 2009/110/EC*".

The fact that e-money is something other than a payment service is perfectly illustrated by the MiCA Regulation when it establishes a similarity of "function" (stabilisation of their value) between crypto-assets, which refer to an official currency in order to maintain a stable value, and e-money and when it allows holders of *e-money tokens to* claim their repayment, in the same way as e-money.[102]

Nevertheless, the trend seems to be towards the 'alignment' of concepts, means and instruments. Take, for example, the new PISA framework for the supervision of electronic payments: the various bodies of rules relating to cards, credit transfers, direct debits and e-money have now been replaced by a single framework (the PISA framework) within which electronic payment instruments include *"payment cards, credit transfers, direct debits, e-money transfers and digital payment tokens*"[103] .

(c) **What remains to be clarified**

Firstly, the *very concept of electronic money has* yet to be defined, otherwise we will continue to refer to an ill-defined object.

In fact, despite the time that has elapsed since EMD2, we are still unable to correctly qualify a product or service that straddles the boundary between payment services and electronic money.

Is it the 'pre-payment' that fundamentally characterises electronic money? Is it the reserve of monetary value or purchasing power[104] ? Is it rather its (conventional)

---

102 So much so that one might ask what the difference is between electronic money and electronic money institutions from the point of view of the legal definition, which is fundamentally different because it has the obligatory character of a discharge, MiCA Regulation.

103 ECB, "*Eurosystem oversight framework for electronic payment instruments, schemes and arrangements*", November 2021, p.3.

104 See G. Blanluet, "La monnaie électronique, valeur monétaire", Revue de droit bancaire et financier no. 2, March 2001, dossier 100018; *and* J. Rochfeld, "Monnaie électronique", RTD civ. 2003, p. 361.

payment acceptance network? Are there other characteristic features and, if so, what are they?

The debate persists and, above all, continues to feed the impression, which is actually a little tiresome, that electronic money is difficult to grasp because of the lack of a clearly and solidly defined concept.

This difficulty is not merely conceptual, as DG FISMA has pointed out:

> *"It has been noted by several stakeholders that users do not perceive a difference between an e-money account and a bank account, both PIs and EMIs are both issuing payment cards, and e-money entities are increasingly acting as providers of payment services."*[105].

However, the intention of EMD2 was clear:

> *"It is appropriate to introduce a clear definition of electronic money in order to make it technically neutral. That definition should cover all situations where the payment service provider issues a pre-paid stored value in exchange for funds, which can be used for payment purposes because it is accepted by third persons as a payment"*[106] .

Perhaps we don't always know what it is, *but does electronic money actually serve a purpose*?

This raises the question of the 'usefulness' (practical, concrete, backed up by market models) of electronic money: what can it be used for that cannot be satisfied, in particular, by classifying it as a payment service?

Clearly, the MiCA Regulation offers a formidable rebuttal to those who would be tempted to reply that electronic money serves little purpose after all, other than to cloud people's minds. The MiCA Regulation has the advantage of being able to categorise a whole variety of crypto-assets that will be "*deemed to be 'electronic money'*"[107] and will be subject to the MiCA regime (issuance, redemption, etc.).

This illustrates the idea that, from the outset, electronic money was conceived as a monetary representation suitable for online use; suitable for secure payment over the Internet. This usefulness of "network money" has been perfectly demonstrated by PayPal, which in addition to its solution as such, has developed a genuine

---

105 DG FISMA, op. cit. p. 113.

106 Recital 7 of EMD2.

107 Recital 66 of the MiCA Regulation.

payment scheme, recognised as such by the PISA framework, in the same way as the SCT or SDD schemes[108] .

In this vein, the Banque de France significantly sees electronic money as "*a specific form of money dedicated to transactions*"[109] .

Another original feature of electronic money payments is that they do not require a bank account (or, more accurately, a payment account) in order to thrive, something that the European Central Bank ("**ECB**") was well aware of at the outset: *"A distinguishing feature of transactions carried out with electronic money is that they do not necessarily involve a bank account. This is a fundamental difference between electronic money and access products. With access products, such as debit cards, payments are settled by means of transfers between bank accounts*"[110] .

Be that as it may, these 'positive benefits' must be highlighted to counterbalance what all too often justifies the use of electronic money: its anonymity. When you consider the extent to which anonymity is constantly hounded by AML/CFT regulations, it is easy to see that the days of 'anonymous electronic money' are behind us. If the choice of electronic money were justified solely by the quest for anonymity, it would already be irrelevant.

There is also the recurring question of the distinction between payment accounts and e-money accounts.

Without going into the discussion here, which is the subject of separate developments in this report,[111] is an e-money account (which we now know can be "ibanised") still a payment account? The abovementioned study by DG FISMA notes that there is uncertainty and divergence in the European Union regarding the possibility of combining an e-money account and a payment account.[112] Is an e-money account a payment account only when it is used to execute and receive payment transactions? Can it be used to "store" where a payment account can only

---

108 Cf. ECB, "*List of overseen schemes under the PISA framework*", 4 October 2022.

109 Banque de France, "Paiements et infrastructures de marché à l'ère digital", chap. 1, May 2022, p. 12.

110 ECB, "*Issues arising from the emergence of electronic money*", ECB Monthly Bulletin, November 2000, p.49.

111 See paragraph 7.1.2 below.

112 "*There is for example uncertainty about whether an account combined with a prepaid card with an IBAN number can be defined as an electronic money account or a payment account*", DG FISMA, "*A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*", FISMA/2021/OP/0002. p. 115.

be used to execute? etc.[113] Would an e-money account be more "technical" than a payment account? Could it remain anonymous in this respect? etc.

How are we to interpret the rule, postulated by the SEPA Regulation, that it does not apply "*payment transactions transferring electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions (1), unless such transactions result in a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN*"[114] ?

It should be noted that an opinion emerged in the working group that the recurring difficulty in understanding electronic money stems from the fact that two very different models of electronic money actually coexist:

(i) in the first, which is more Anglo-Saxon, electronic money is difficult to distinguish from scriptural money because, like scriptural money, it is used in an open circuit in an open network of acceptors (universal card payment); the usefulness of classifying electronic money would be that it would allow the account that collects it to keep the funds, unlike a payment account which, by definition, is only used to carry out payment transactions. Until a recent response from the EBA in its Q&A, there was uncertainty as to whether funds could be kept on a payment account in the form of a balance in the absence of a predefined payment order.[115] According to this model, electronic money stored in this way on an account offering functionalities comparable to those of a payment account within the meaning of the PAD Directive would be such as to imply the existence of a payment account;

(ii) the other, closed-loop model, is similar to the PayPal account or closed-loop (staged) digital wallet, which only allows e-money transactions if both the payer and the acceptor have an account with PayPal.[116] This is the hypothesis where the receipt of electronic money implies a centralised accounting system with the issuer of the electronic money. Although limiting, this approach nevertheless reflects the intrinsic characteristic

---

113 On the distinction between payment accounts and electronic money accounts, see ECB, "*ECB Opinion of 5 December 2008 on a proposal for a directive on the taking up, pursuit and prudential supervision of the business of electronic money institutions*" (CON/2008/84).

114 Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and commercial requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009, Article 1(2)(f).

115 See EBA, Q&A n°2018_4221.

116 See Section 7.7.1.7.1.2 Specific electronic money account and payment account.

requirements of electronic money, in particular the need for any holder of electronic money, whether payer or payee, to be bound by a contract with the electronic money issuer and for the electronic money to circulate between electronic money media in accordance with the rules defined by the issuer. The electronic money medium, whether physical or dematerialised, would not have the functionalities characteristic of a payment account.

2.4. HCJP recommendations

Merger or not, the priority would be to redefine electronic money, so that we finally know what we are referring to and what we want to do with it.

> **Recommendation No. 2:** The HCJP recommends the revision of the concept of electronic money, not only because the current definition remains abstruse, but also so that it can be used for the innovations currently underway, in particular concerning crypto-assets, but more broadly the new "payment value chains".

Now that there seems to be a consensus in favour of a merger between EMD2 and PSD2, it is still important to agree on the scope (all or part of e-money law) and the nature of this merger (purely technical or recomposing payment services and e-money law).

This opportunity would also make it possible to merge the authorisations of PIs and EMIs, thereby correcting the excessive regulatory arbitrage that currently results in certain countries (*e.g.*, Lithuania, Malta, etc.) being champions of electronic money, for no apparent reason other than that they are very welcoming to EMIs.

> **Recommendation No. 3:** The HCJP recommends: (i) firstly, that the merger should make it possible to bring together, in a single body of rules set out in a single text, the entire regime common to electronic money and payment services (law on payment transactions and payment service contracts); and (ii) secondly, that a single category of payment service providers should be created (the "payment and electronic money institutions" or "PEMIs") subject to common prudential provisions, customer protection provisions, etc., subject to a few exceptions (minimum capital, redemption of electronic money, etc.).

It turns out that the economic and legal models for electronic money oscillate between a universal means of payment (prepaid cards) and, on the contrary, a closed system of payment between affiliates. Is it conceivable to maintain these two uses with a common undifferentiated regime? Or should we make a clear distinction

between them and apply special rules (for example, a system of anonymity limited to closed-circuit electronic money)? Added to this is a fundamental issue, given that the *Paysera* case law has established the redeemability of electronic money as a substantial feature: how can this be guaranteed within a universal acceptance network?

> **Recommendation No. 4:** The HCJP recommends that a clarification be made between the open universal payment model and the payment system exclusively between affiliates. Without such clarification, there is a risk of persistent confusion between payment services and electronic money or the potential emergence of practical challenges (e.g., reimbursement) that may become insurmountable.

The "medium", the "form" in which the monetary value constituted by electronic money is stored deserves to be clarified, which neither EMD1 nor EMD2 have done.

> **Recommendation No. 5:** The HCJP recommends that the future text contain a definition of the electronic money medium, for at least two reasons: (i) electronic money is often confused with the medium (payment card, payment account) which stores it, thereby hindering its identification and qualification; and (ii) forward-looking, a definition of the electronic money medium capable of embracing the future *e-money* tokens of the MiCA Regulation.

3 TERRITORIAL SCOPE OF THE PSD2

3.1 Issues related to the question

Identifying the location of a payment service (and, in particular, the question of when a payment service should be considered to be provided or not within the territory of a given EU Member State) raises a number of difficulties due to the fact that most of the time such services are intangible, delocalised and/or provided at a distance. The situation is even more critical given the increasing digitalisation of financial services.

The challenges of locating payment services are real and arise at two levels:

(i) *in respect of intra-Community services*: as regards European passports, the question of whether a payment service is provided on a cross-border basis within a Member State is crucial in order to determine whether such a service falls under the freedom of establishment or the freedom to provide services;

(ii) *in respect of services provided by a third-country provider*: the question arises as to whether a payment service provided by a third-country provider to a user (in other words, a customer) domiciled in a Member State is subject to the rules of PSD2 and therefore triggers the requirement for that provider to obtain authorisation[117]. In other words, the question is whether the mere fact that the customer is domiciled within the EU is sufficient to consider that, in the absence of any other geographical connection, such services are provided within the EU and are subject to the provisions of PSD2. The stakes underlying this clarification are particularly high given that, criminal sanctions are provided for in some Member States such as France for breaching monopolies, including the monopoly on payment services.[118] It should also be noted that, in this case, the application or non-application of the PSD2 framework to a given service provider has consequences that go beyond the question of authorisation, since it is the applicability of the substantive rules of PSD2 themselves (and therefore the protection of the payment service user) that is at stake. Such an assumption is however not theoretical. This is the case, for example, of an expatriate who has opened an account abroad and who, once he returned to his country of origin, has not closed his account and continues to use it (for example, to continue repaying a mortgage, pay the charges for his flat, etc.). Apart from this anecdotal situation, many companies with activities abroad generally open

[117] As a payment, credit or electronic money institution.

[118] See article L. 521-2 of the Financial Code.

accounts abroad for the needs of their international activities, in order to access cash and foreign currency liquidities (for example, dollars) with foreign banks that do not have regulated establishments within the EU. Sometimes banks located in the EU may also use correspondent banks established in third countries on behalf of their customers. In all these cases, the third-country bank is likely to provide one or more payment services to a customer domiciled in a Member State. Does this entail that the foreign bank is in breach of the PSD, particularly in terms of its obligation to be authorised as a PSP? The issue of determining the location of the provision of payment services within the European Union has, for example, been highlighted recently with Brexit in relation to payment services provision contracts which were entered into before Brexit but continued after it. While the validity of these contracts, assessed at the time they were entered into before Brexit, was not called into question, their performance after Brexit (and therefore following the loss of the European passport) has raised difficulties.[119] These European situations have been analysed by the HCJP. In particular, as regards the bank accounts/payment accounts and the corresponding banks, the HCJP considered that the regulated services (receipt of deposits, payment services, etc.) were not provided on the territory of the Member State in which the customer is domiciled.[120]

3.2. **What is the current legal regime?**

A review of the rules of positive law applicable to payment services, whether at European level or Member State level concludes that there are no clear criteria for the localisation of the provision of a payment service. Supervisory practices vary from one Member State to another, leading to disparate application of the rules arising from PSD2.

3.2.1 *In the PSD2*

While PSD2 expressly specifies its territorial application, it does not set any criteria for determining precisely when a payment service should be considered as being provided within the European Union or on the territory of a given Member State.

---

119 European Banking Authority opinion on issues relating to the UK's departure from the European Union, 12 October 2017, available here; EBA calls on financial institutions to finalise preparations for the end of transitional arrangements between the EU and the UK, 29 July 2020, available here.

120 HCJP, Brexit report, banking and investment services activities, 15 October 2018, available here.

For example, Article 2.1 of PSD2, which sets out the scope of the directive, simply states that: "*This Directive applies to payment services provided within the Union*".

Articles 2.2 to 2.4 of the PSD2 indirectly consider the situation where a payment service is provided by a payment service provider outside the European Union, but only by reference to the situation where the other provider is located within the European Union, in order to determine the scope of application of certain rules. For example, when a consumer residing in the EU pays a merchant established in a non-EU country for his purchases, the merchant's payment service provider, generally established itself in the merchant's country (the PSP acceptor), provides the payment service to the non-EU merchant ("*one leg out"* transaction). Conversely, when a consumer residing in a non-EU country pays a merchant established in the EU for his purchases, the consumer's payment service provider (PSP payer) in the non-EU country provides the payment service to the consumer outside the EU. In both cases, the payment service provider of the EU resident in the first example and the payment service provider of the merchant established in the EU in the second example, provide the payment service in the EU. The cross-border element in these two examples is the payment flow from one payment account to another (and not the provision of the payment service, which remains domestic in nature).[121] Nevertheless, the text does not resolve the issue of when a payment service should be considered to be provided by a third-country provider to a payment service user in the territory of a Member State of the European Union.

3.2.2. *In Member States' legislation*

In the legislation of the consulted Member States, it appears that there are no provisions of a normative nature (law, regulation, decree, etc.) laying down rules of connection to the territory concerned. However, it can be noted that in several Member States (Italy, Spain and France), the rule of solicitation is used by the supervisory authorities. In other countries, such as Spain and Luxembourg, the location of the characteristic performance is also taken into account, as is the location of the payment account (Germany).

As demonstrated in the above-mentioned HCJP report on Brexit, the issue of the territorial scope of monopoly rules is not limited to the PSD. Other sectoral regulations are also affected. It is therefore interesting to compare these texts in order to check whether such an issue is resolved appropriately.

---

[121] See EBA, "*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*", EBA/Op/2022/06, 23 June 2022, available here.

3.2.3. *Comparison with other European sectoral texts*

For other financial services, the question seems to arise in similar terms. While the location of other financial services entails the same issues (relating to passporting and authorisation), the European supervisory authorities themselves note that no definition of cross-border provision of services is included in any of the revised level 1 texts.[122] They emphasise the absence of clear criteria for determining the place where the service is provided, even though this is a key issue.[123]

Although Directive 2002/65/EC of 23 September 2002 concerning the distance marketing of consumer financial services, which covers the cross-border provision of financial services, should be mentioned, this text does not make it possible to determine the point at which it should be considered that a financial service is provided on the territory of the Union or of a given Member State.

That being said, it seems useful to consider the third country regime provided for in the MiFID/MiFIR package. This regime sidesteps the question of territoriality analysed from the angle of objective material criteria of geographical nexus (multi-criteria analysis based mainly on the characteristic performances of the service in order to determine the place where this performance is carried out), which may be considered not relevant in the context of the provision of cross-border investment services,[124] by providing for an alternative legal mechanism based on reverse solicitation (see Appendix V). Other recent texts contain provisions relating to services provided by companies from third countries.

Based on the analysis of the other European sectoral texts mentioned in the table above, it is interesting to note that recent texts (or draft texts) follow the path paved by the MiFID/MiFIR package by applying the reverse solicitation regime (MiCA Regulation and CRD6). The solutions adopted for EMIR, CSDR and AIFMD are, however, specific to the services regulated by these texts and their solutions do not seem transposable to the case of payment services.

---

122 Joint Committee of the European Supervisory Authorities, "*Report on the cross-border provision of financial services*", 9 July 2019, JC/2019-22, available here. Para. 66: "*there is no definition of cross-border provision of financial services in any of the Level 1 texts reviewed.*"

123 *Ibid*. para. 66.

124 Comité des établissements de crédit et des entreprises d'investissement (CECEI), "*The freedom to provide services in the area of investment services"*, 20 November 1998, spec. p. 3. Certainly in the context of the provision of cross-border services under the passport (but the reasoning also applies in the context of services provided from a third country.

3.3. **Available options**

If one wishes the PSD to incorporate specific provisions setting out the criteria by which the provision of a cross-border payment service triggers the authorisation requirement, several options are available:

3.3.1 *Place of execution of the characteristic performance*

Applications	**Description**	**Benefits**	**Disadvantages**
Banking services. The place of execution of the characteristic performance has been retained in banking matters by case law and recommended by the HCJP in the specific context of Brexit as regards payment services (more specifically, as regards the opening and operation of payment accounts).[125]	This approach consists of using the place where the characteristic performance is carried out as the determining territorial nexus criterion of a service. By applying a multi-criteria analysis of the geographical location of the execution of the characteristic performance, a given payment service should not be considered to be provided on the territory of the European Union or of a given Member State if the characteristic performance of the service is located	Legal certainty based on the identification of objective criteria. An approach tailored to professional or institutional clients with offices abroad or whose activities are focused on foreign markets.	This approach is potentially unsuitable for dematerialised services. In the case of payment services, this approach could lead to the view that, where the payment service is provided from a payment account and the payment account is held at the head office of the third-country provider, the service would systematically be provided outside the territory of the EU.[127] Furthermore, in the case of payment services that are not provided in conjunction with another payment

[125] HCJP, "Report on Brexit, banking and investment services activities", 15 October 2018, p. 22. In this report, the working group considered that, with regard to "*correspondent banking*" contracts, the services performed by the entity located in the United Kingdom should not fall within the geographical scope of the banking and payment services monopolies, thus allowing for the continued performance of this contract post-Brexit and that, in the absence of case law, the same approach should apply with regard to the opening and operation of a payment account.

[127] The same criticism has been made in relation to investment services, *see* above.

	outside this territory. The determination of this place of execution of the characteristic performance could take into account a certain number of criteria depending on the payment service concerned (such as the location of the payment account, the place where the means of payment are issued and made available, etc.), which should in principle point to the place of establishment of the payment service provider.[126]		service (i.e. services no. 6, 7 and 8), the approach based on characteristic performance does not seem appropriate, as the only objective criteria will be limited to the country of residence of the service provider and his customer (other criteria, such as the place of conclusion of the contract, are not really appropriate for contracts concluded online).[128]

3.3.2. *Soliciting the customer*

Applications	Description	Benefits	Disadvantages
Approach adopted by MiFID/MiFIR, MiCA and CRD 6 by reverse application of the "reverse solicitation" exception.	This approach focuses on the place where the customer is solicited. Thus, if a payment service provider solicits a customer within the EU, either directly or through a third party acting on his	Objective and predictable criterion, and consistent with the idea that the customer protection regime is not intended to prevent customers from accessing services	Risk of circumvention through the use of standard contractual clauses (although this risk has been mitigated by ESMA's MiFID/MiFIR policy).

[126] See on this point, in particular HCJP, "Report on the accessibility of the French market by UK banking and financial institutions in a post-Brexit environment", 7 November 2017, p. 13.

[128] Can also give rise to circumvention strategies by artificially locating the characteristics of the service or operation outside the territory of the EU That said, if the connection to a given territory appears to be artificial, it is likely that the judge will reject such a connection.

	behalf, the payment service should be considered to be provided within the EU, regardless of whether the characteristic performance of the contract takes place outside the EU. Conversely, if the business relationship with the third-country payment service provider and the subsequent provision of payment services are entered into exclusively on the customer's initiative (reverse solicitation), without any prior solicitation by the provider in the territory concerned, these payment services will be considered as being provided outside the EU, even though the characteristic performance of the contract will take place within the EU.	provided from abroad. Criterion adapted to professional or institutional customers seeking the provision of payment services by third-country providers as part of their international activities (access to foreign payment/exchange systems, international cash management solutions, etc.). This approach would have the advantage of contributing to a cross-sector harmonised third country regime, in particular through the development of a doctrine by the joint ESA committee.	This solution is not suitable for retail customers. Difficulty in proving the customer's exclusive initiative.

3.3.3. *Customer's address*

Applications	Description	Benefits	Disadvantages
Approach adopted by EMIR, as interpreted by the European	The mere fact that the customer is domiciled in the	This criterion is simple to implement	This criterion is unsuited to professional or

Commission. Position implicitly adopted by the EBA in its press release on the consequences of Brexit for the provision of payment and e-money services.[129]	EU is enough to trigger the authorisation requirement for a third-country service provider providing a cross-border service from its head office.	and predictable. Very protective and suitable for retail customers.	institutional customers seeking payment services from third-country providers as part of their international activities. The main consequence of such an approach would be to deprive such customers of access to international payment services provided by third-party providers, particularly (but not exclusively) in relation to payments in foreign currencies. In the area of UK clearing houses and payment systems, this is why ESMA has extended the transitional regime under EMIR and why various Member States have "transposed" recital 7 of the SFD. Contrary to the principle according to which the aim of regulations is not to prohibit customers from using the service provider of their choice (including foreign service providers),

[129] EBA press release, "EBA calls on financial institutions to finalise preparations for the end of transitional arrangements between the EU and the UK", 29 July 2020.

			but to prohibit third-country companies from undertaking marketing or sales activities on EU territory or aimed at EU customers without authorisation.

3.4. **HCJP recommendations**

The criterion of soliciting a customer domiciled in an EU Member State is simple to implement and protects customers, particularly non-professional customers. This criterion is also consistent with third-country regimes in recent sectoral texts. These are the reasons why the HCJP recommends retaining the solicitation of customers domiciled in the European Union as a territorial nexus criterion for the revision of PSD2.

> **Recommendation No. 6:** The HCJP recommends adopting client solicitation in the European Union as a territorial nexus criterion for the revision of PSD2.

4. MATERIAL SCOPE OF PSD2 - COLLECTION OF FUNDS ON BEHALF OF THIRD PARTIES

4.1. Issues relating to the inclusion of the collection of funds on behalf of third parties in the scope of the PSD

Traditionally, we have known been familiar with the activity of amicable debt collection on behalf of third parties, which has been governed by a number of rules since 1996[130]. With the rise of online marketplaces, crowdfunding platforms and digital asset exchange platforms, this activity is now carried on informally by these online marketplaces, which collect funds on behalf of their users (for example, when a consumer buys goods on an online marketplace, the consumer pays the price to the marketplace, which then pays it back to the merchant).

When the PSD came into force in 2009, the question arose as to whether this activity could be subject to the directive.[131] The ACPR[132] and the case law[133] have answered this question in the affirmative.

Although it does not in itself constitute a payment service within the meaning of the PSD, nor is it the subject of specific provisions in this directive (or in the Financial Code), the activity of collecting payments on behalf of third parties may, according to the ACPR, involve the provision of one or more of the payment services mentioned in Article L. 314-1 of the Financial Code. With regard to marketplaces, which initially collect sums from buyers on behalf of merchants and then pay them back to those merchants, after deducting their commission where applicable, the ACPR stated that their activity could involve the provision of two payment services: the acquisition of payment orders[134], on the one hand, and, on the other hand, the execution of transfer transactions associated with the

---

130 Decree no. 96-1112 of 18 December 1996 regulating the activities of persons engaged in the amicable collection of debts on behalf of third parties. Now codified in the Code des procédures civiles d'exécution ("**CPCE**"), in articles L.124-1 and R. 124-1 to R. 124-7.

131 P. Storrer, "L'encaissement de fonds pour le compte de tiers vaut-il fourniture de services de paiement?", Revue Banque no. 777, Nov. 2014, p. 86.

132 "La régulation des nouveaux intervenants du marché des services de paiement", Revue de l'ACPR n°21, January-February 2015, p.6. See also, ACPR website: "Qualifier mon activité", question 5: "dès lors que j'encaisse des fonds, quel statut dois-je adopter?", and ACPR and AMF, "S'informer sur le nouveau cadre applicable au financement participatif (crowdfunding)", 30 Sept. 2014 and updated on 26 August 2016 and 9 May 2017 (companies operating a crowdfunding platform must, when collecting funds, be authorised as a payment institution or be registered as a payment service provider agent).

133 Regarding a *Bitcoin* exchange platform: CA Paris 26 Sept. 2013, no. 12/00161, *SAS Macaraja c/ SA Crédit Industriel et Commercial*.

134 Service no. 5 of Annex I of the PSD2 and article L. 314-1, I, 5° of the Financial Code.

management of a payment account,[135] or even the money remittance service (in the absence of a payment account opened in the name of the payer or payee in the platform's books)[136]. Consequently, according to the ACPR, payment services are provided by the service provider if the funds are, on the one hand, collected or received on a payment account belonging to the service provider and, on the other hand, collected by the service provider on behalf of a third party (in other words, the service provider does not receive funds for itself, but as an intermediary with the aim of transferring them to their true recipient). Conversely, if one of the conditions is missing, then no payment should be made.[137]

Consequently, only a special legislative text taking precedence over the provisions of the PSD transposed into the Financial Code or a derogation expressly provided for by the PSD[138] can allow the application of the payment services regulations to be waived.[139] Alternatively, the service provider may engage in a partnership with a PSP and register as an agent of that PSP ("**APSP**").[140]

---

135 Service No. 3(c) of Annex I of the PSD2 and Article L. 314-1, I, 3°(c) of the Financial Code. Note the subtle difference in wording between the French transposition text and that of the French version of the Directive, which does not exist in the French-language transpositions of the PSD2 (in Belgium and Luxembourg). The French transposition seems to be able to give a much broader scope to this payment service.

136 Article L. 314-1, II, 6°. See also, "La régulation des nouveaux intervenants du marché des services de paiement", Revue de l'ACPR, *ibid*.

137 "La régulation des nouveaux intervenants du marché des services de paiement", Revue de l'ACPR, *ibid*.

138 These are the exclusion relating to the commercial agent (Article 3(b) of the PSD, transposed into Article 314-1, III, 3° of the Financial Code) and the exemption relating to the limited network of acceptors or the limited range of goods or services (Article 3(k) of the PSD2, supplemented by "Guidance on the exclusion relating to "limited networks" under PSD2" published by the EBA on 24 February 2022 (EBA/GL/2022/02) and Position 2022-P-01 having been published by the ACPR on 20 July 2022 concomitantly with its notice of compliance with the EBA Guidance, replacing Position 2017-P-01).

139 According to the ACPR, these are certain legislative texts that provide specific professions such as lawyers, notaries, estate agents or travel agents with an *ad hoc* legal framework for collecting funds on behalf of third parties. In the absence of a specific text, only one exclusion or exemption from authorisation provided for by the PSD allows the activity to continue without authorisation: the exclusion relating to commercial agents, or the exemption relating to limited networks or a limited range of goods and services.

140 Spec. article 19 of the PSD2, transposed into articles L. 523-1 et seq. of the Financial Code.

This approach was strongly criticised by academics,[141] especially as at the time, neither the EBA nor any other national authority competent for payment services in another Member State had officially positioned themselves on this issue.[142]

Moreover, as the ACPR itself points out, this approach goes beyond internet platforms and is intended to encompass any situation in which a person pursues a collection activity on behalf of a third party[143]. This would be the case, for example, of a finance company[144] which, as part of the syndication of its financing, acts as a credit agent on behalf of the syndicate. The case of the security agent, acting on behalf of the creditors who have appointed it to take out, register, operate and enforce securities guaranteeing their claims, and collecting the proceeds of the execution of the securities on their behalf, certainly raises questions. Do the provisions of articles 2488-6 and seq. of the French Civil Code,[145] which do not impose any conditions relating to the status - regulated or otherwise - of the agent, constitute a special legislative text that prevails over the PSD? Or does the fact that the security agent acts in its own name (and not in the name of the creditors) for the purposes of enforcing the security - and therefore of collecting the resulting funds[146] - suffice to consider that it is not acting as a mere intermediary and is therefore outside the scope of the PSD?

More concretely, the question of the status of debt recovery companies should also be raised. In fact, their profession is not regulated as such, only the activity of debt collection on behalf of third parties is regulated by the CPCE.[147] However, the

---

141 M. Roussille, "*Marketplaces* et services de paiement: jusqu'où ira l'impérialisme de l'ACPR ?", Revue de droit bancaire et financier, nov.-déc. 2014, focus 23 and T. Bonneau, "Une société qui utilise un compte bancaire sur lequel transitent des *bitcoins* est-elle un prestataire de service de paiement?", JCP E n°8, 20 févr. 2014, 1091.

142 See paragraph 4.4.2..

143 "La régulation des nouveaux intervenants du marché des services de paiement", Revue de l'ACPR, *ibid*.

144 Authorised by the ACPR (article L. 511-1-II of the Financial Code) to carry out credit transactions on a regular basis and on its own account (article L. 511-10-II of the Financial Code). To provide payment services, a finance company must also obtain authorisation as a credit institution or be authorised as a payment institution.

145 The case of collection on behalf of third parties is not expressly provided for in these provisions, but necessarily follows from the authority given to the agent to enforce security on behalf of creditors (see Fédération nationale de l'information d'entreprise, de la gestion des créances et de l'enquête civile, "Activité de recouvrement de créances": no mention is made of this in the PSD2). Also: https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/recouvrement-creances.

146 It should be noted that the funds collected in this way form assets assigned to the agent's mission, distinct from his own assets (article 2488-6 of the Civil Code) and must be paid back by the agent to the creditors who appointed him.

147 Cf. supra, footnote no. 130. Indeed, this is how debt collection professionals understand their regulatory obligations (FIGEC, "Le recouvrement de créances, enjeux et perspectives", White

framework laid down by this code is open to any person, including those acting for non-professional, occasional or ancillary purposes: "*The activity of natural or legal persons not subject to a professional status who, on a regular or occasional basis, even on an ancillary basis, carry out collection of debts with the debtor's agreement on behalf of others, is carried out under conditions laid down by decree in the Conseil d'Etat*". The relationship between this text and the PSD is uncertain, since the CPCE is clearly not a special legislative text that takes precedence over the provisions of the PSD as it sets out a general auxiliary framework applicable in the absence of any professional status. Consequently, the provisions of the CPCE and those of the PSD appear to have the same purpose, namely, to regulate the activity of collecting funds on behalf of third parties when it is not covered by a regulated professional status.[148]

In addition, the application of the PSD2 rules to the activity of collecting payments on behalf of third parties will have to be coordinated with those arising from the Credit Servicers Directive, which is due to be transposed into French law by 29 December 2023.[149] This directive provides a framework for credit management activities, which include, in particular, "*collecting or recovering from the borrower, in accordance with national law, any payments due related to a creditor's rights under a credit agreement or to the credit agreement itself*"[150] and makes credit servicers subject to an authorisation requirement.[151]

There are many important issues linked to the submission of the activity of collecting funds on behalf of third parties, in view of the consequences arising from the application of PSD2. These include:

(i) the requirement for authorisation (as a payment institution, credit institution or, where applicable, an electronic money institution); and

(ii) where the service provider is deemed to hold a payment account on behalf of the creditor (where service No. 3 in Annex I to PSD2 is identified), the

Paper, November 2014, spec. p. 19). See also, DGCCRF, "Recouvrement amiable, les règles à connaître" (https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/recouvrement-creances).

148 It should be noted in passing that the ACPR does not cite these provisions among those that could take precedence over those of the PSD (see footnote no. 132).

149 Directive (EU) 2021/2167 of the European Parliament and of the Council of 24 November 2021 on credit managers and credit purchasers and amending Directives 2008/48/EC and 2014/17/EU.

150 Article 3(9).

151 Article 4(1).

obligation to apply strong authentication (SCA) of the account holder,[152] as well as the facilitating of the provision of account information and payment initiation services on[153] accounts (open banking),[154] and the compliance with the resulting technical constraints.[155]

4.2. What is the current legal regime?

4.2.1. *In the PSD2*

As indicated above, the collection of funds on behalf of third parties is not an activity that falls clearly within the scope of PSD2. In any case, it is not a payment service listed in Annex I of the Directive. At most, it is envisaged indirectly by Recital 9, mainly from the point of view of money remittance: " *Money remittance is a simple payment service that is usually based on cash provided by a payer to a payment service provider, which remits the corresponding amount, for example via a communication network, to a payee or to another payment service provider acting on behalf of the payee. In some Member States, supermarkets, merchants and other retailers provide to the public a corresponding service enabling them to pay utilities and other regular household bills. Those bill-paying services should be treated as money remittance, unless the competent authorities consider the activity to fall under another payment service*".

However, subsequent to the ACPR's 2015 publication,[156] the EBA published, between 2021 and January 2023, three Q&A confirming the French position,[157] under which it considers that third-party collections should be classified as a payment service under Article 4(3) of PSD2 and Annex I thereto, unless the exclusion in Article 3 of PSD2 relating to commercial agents applies. The EBA points out that the activity of collecting payments on behalf of third parties may, depending on the contractual arrangements and flows analysed, constitute the activity of money remittance (Article 4(22) of the PSD2, payment service No. 6 of Annex I to the PSD2), or any other payment service, such as the acquisition of payment transactions (Article 4(44) of the PSD2, payment service No. 5 of Annex I to the PSD2).[158] It is therefore certain that the collection of funds on behalf of

---

152 Article 97(1)(a) of the PSD2.

153 Respectively, services no.ˢ 8 and 7 of Annex I of the PSD2.

154 Articles 66 and 67 of the PSD2.

155 Provided for in Delegated Regulation 2018/349.

156 See above footnote no. 132.

157 EBA, Q&A n°2020_5216, n°2020_5355 and n°2020_5099 (published on 6 January 2023).

158 It is interesting to note that the EBA does not mention (but does not exclude) service no. 3 in Annex I of the PSD2. To the best of our knowledge, only the ACPR identifies this service first

third parties is a payment service according to the EBA, which may fall under one or more of the categories provided for in Annex I depending on the circumstances of the case and the type of activity. It also interprets the exclusion of commercial agents textually. This exclusion can only apply if the agent is authorised by the beneficiary to negotiate or conclude the sale of goods or services and if he is not also acting on behalf of the payer.[159] The exclusion therefore only applies in limited cases.

The EU Regulation of 7 October 2020[160], which establishes a harmonised legal framework for crowdfunding in the EU, specifies for its part that a crowdfunding service provider that provides payment services in connection with its crowdfunding services must also be authorised as a PSP.[161]

4.2.2. *In the legislation of the Member States*

A multi-jurisdictional analysis was carried out in four countries to determine whether the Member States in question consider that the activity of collecting funds on behalf of third parties falls within the scope of the PSD2[162]. First, in none of these Member States has the competent authority taken an official position and no case law has been identified. Second, practitioners seem to consider that this payment activity is likely to fall within the scope of PSD2, in particular because of the EBA's Q&A, which the competent national authorities will probably follow. Third, the precise identification of the payment services concerned is highly uncertain, although the money remittance service (service No. 6 in Annex I of PSD2) appears to be the most obvious choice.

Details of the multi-jurisdictional analysis can be found in the appendix to this document.

4.3. **HCJP recommendations**

In conclusion, it appears to the working group members that, in the absence of PSD provisions and taking into account the position expressed by the EBA and certain competent national authorities such as the ACPR, the activity of collecting funds on behalf of third parties should be considered as falling within the scope of the

---

and foremost (along with service No. 5 in Annex I of the PSD2) in the context of collection on behalf of third parties.

159 EBA, Q&A n°2020_5355.

160 Regulation 2020/1503 of 7 October 2020 on European providers of participatory finance services for entrepreneurs, and amending Regulation 2017/1129 and Directive 2019/1937.

161 Recital 29 of the regulation.

162 Germany, Spain, Italy, Luxembourg and Poland.

provision of payment services under the PSD. However, the working group also notes that, on the *one hand*, this position remains generally unknown to the players who usually carry out this activity; on the *other hand*, there is a degree of vagueness as to the question of determining which payment services are relevant,[163] in the absence of sufficiently precise indications from the authorities,[164] in particular with regard to the consequences attached to the classification of certain services (in particular, in terms of obligations linked to open banking) which may appear disproportionate in relation to the objectives of the PSD2; and, *finally*, the scope of the EBA's position with regard to activities linked to debt collection or to economic activities involving the collection of funds on behalf of third parties but which are not intended to fall within the scope of the regulations on payment services (the need for regulation of intermediaries pursuing the activity of collection on behalf of third parties could be satisfied by the introduction of a specific legal framework).

Recommendation No. 7: The HCJP recommends: (i) to clarify the fact that the activity of collecting funds on behalf of third parties involves the provision of identified payment services, so that the qualification is clear to the actors; and (ii) give the EBA the power to draw up regulatory technical standards in order to define the conditions under which the identified services apply, including non-exhaustive examples where appropriate.

Recommendation No. 8: The HCJP recommends indicating that Member States may provide for exceptions concerning identified professions or activities, which will mean, in the case of France, clarifying the situation of certain professional activities falling within the scope of the CPCE.

163 It should be noted in this respect that, as the EBA points out, there is a debate on the distinction between two payment services that seem difficult to distinguish from one another: the transfer associated with a payment account (covered by service No. 3(c) of Annex I of the PSD2) and the money remittance (service No. 6 of Annex I of the PSD2)(EBA, *op. cit*, § 5 to 9, pp. 8 and 9), while the first requires the opening of a payment account, the other does not, it being understood that the plasticity of the notion of payment account makes this distinction more difficult to grasp.

164 The ACPR's recent efforts to make its positions easier to understand should be noted, particularly on its website: "Qualifying my activity", question 5: "As soon as I collect funds, what status should I adopt? The ACPR analyses the models presented on a case-by-case basis.

5. EXCLUSIONS FROM THE SCOPE OF THE PUBLIC SERVICE DELEGATION - TECHNICAL SERVICE PROVIDERS (TSPS)

5.1. Issues relating to the exclusion of the provision of technical services from the scope of the PSD2

As part of the payment services they provide to their customers, many PSPs use technical service providers ("**TSP**"), which are often unregulated entities operating in the payment services ecosystem. The European Commission notes that technical services include, in particular, IT maintenance, the implementation of strong authentication services (SCA) or unified API gateways and hubs.[165]

These TSPs may intervene in a visible way ("front end" intervention) between the payment service users and the PSP by offering technological solutions enabling the PSU to make payments online or at the point of sale (POS) via electronic payment terminals. Others may also act as subcontractors to a PSP and are not necessarily visible to the PSU ("back-end" operations).[166] Whatever the formula, their activities are often intrinsically linked to the provision of payment services by PSPs to payment service users and may give rise to numerous risks associated with their involvement in the payment chain. Risks relating to privacy and data protection, competition and cybersecurity may arise from a "front end" perspective, while the financial stability of the players may be affected from a "back end" perspective.[167] There is a risk of contagion between unregulated entities (TSPs) and PSPs. For example, the operational and/or financial problems of a TSP could lead to a suspension of the provision of services by a PSP.[168]

The introduction of open banking by PSD2, through two new payment services, the payment initiation service (service No. 7, Annex 1 of PSD2)[169] and the account information service (service No. 8, Annex 1 of PSD2)[170], has encouraged a growing number of players to work with PSPs to offer technical services. In fact, although payment initiation service providers (PISPs) and account information service providers (AISPs) now fall within the scope of PSD2, many other technical service providers remain outside the scope of PSD2, even though technological developments have blurred the line between technical services and payment

---

165 DG FISMA, "*A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*", FISMA/2021/OP/0002, February 2023, p. 36.

166 DG FISMA, *op. cit.* p. 104.

167 *Ibid.*

168 DG FISMA, *op. cit.* p. 37

169 In France, article L. 314-1 II n°7 of the Financial Code.

170 *Ibid*, article L. 314-1 II n°8 of the Financial Code.

services. This is particularly true as the traditional boundary drawn by the handling or coming into possession of payment service users' funds by PSPs in respect of traditional payment services under PSD1 is no longer relevant with the new services introduced by PSD2, which do not involve any handling or coming into possession of payment service users' funds.[171]

The EBA and the European Commission[172] have identified a number of TSPs whose inclusion or non-inclusion in the scope of PSD2 raises questions.[173]

These include, in particular, major technology services companies such as Apple, Google, Samsung and Tencent, which provide a service (known as "X-Pay")[174] consisting of virtually replicating, on behalf of the issuing PSP, the payment card issued by that PSP in the smartphone of the card issuer's customer.[175] Other technical service providers may also be involved in the payment chain, in particular by providing technical solutions relating to the initiation, acquisition or processing of payment orders. The boundary between technical services and payment services (including, in particular, payment initiation) has become porous, particularly in cases where the company providing the technological service controls the technical process of initiating the payment order and authenticating the payment service user.[176] This boundary is made even more theoretical by the definition of payment instrument as interpreted by the CJEU.[177] Although some of these companies have regulated entities authorised to provide payment services in the EU,[178] these

---

171 On the contrary, the PSIC is prohibited from holding the payer's funds in connection with the provision of the payment initiation service (article 66(3)(a) of the PSD2).

172 EBA, "*EBA's response to the Call for advice on the review of PSD2...*", DG FISMA, *op. cit.*

173 Payment gateways, digital wallet providers, card payment schemes, processing entities, etc.

174 Examples include ApplePay (https://www.apple.com/fr/apple-pay/), GooglePay (https://pay.google.com/intl/fr_fr/about/), SamsungPay (https://www.samsung.com/fr/apps/samsung-pay/) and WeChatPay (https://pay.weixin.qq.com/index.php/public/wechatpay), which is limited to Chinese customers.

175 This is referred to as tokenisation of the card, or the creation of a digital version of the payment card. See DG FISMA, *op. cit*, p. 104: "*More and more (technical) service providers are engaging in the payment transaction value chain, but are not regulated under PSD2. Card wallets in the form of mobile applications (most often applications supported by Google, Apple, or Samsung) provide an interface for initiating card payment transactions at POI. These services are based on the tokenised card.*"

176 DG FISMA, *op. cit*, *loc. cit.*

177 See below.

178 DG FISMA, *op. cit*. p. 108. One example is Google Payments (two EMEs licensed in Lithuania and Ireland respectively).

companies provide these technological services from entities that do not have appropriate authorisation.

It is also worth noting the existence of payment systems or schemes, in particular by card, such as Visa or Mastercard, which do not appear to be limited solely to the provision of technical services, in particular communication services. Traditionally, card payment schemes, for example, are limited to facilitating the exchange of information between the accepting PSP (i.e., the PSP of the merchant's customer) and the card-issuing PSP (i.e., the PSP of the PSU). However, in recent years, new services have been developed[179] which involve the provision of certain payment services.

Aren't these service providers providing payment services under the guise of simply providing technical services?

5.2. **What is the current legal regime?**

5.2.1. *Front-end service providers*

First of all, PSD2 expressly excludes from its scope "*services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services*."[180] The wording of this exclusion is essentially the same[181] as under PSD1, subject to the addition of new services 7 and 8, which restrict its scope. It should also be noted that this exclusion was substantially provided for in the terms of PSD1 from the outset.[182]

As part of the revision of PSD1, a problem had already been raised between, on the one hand, certain technical services consisting of processing and storing payment data and authenticating data and entities and, on the other hand, the acquisition of payment transactions, which constitutes a payment service (service No. 5, Annex 1

179 See, for example, Visa B2B Connect, available here.

180 Article 3(j) of the PSD2, transposed into Article L. 314-1 III, no. 7 of the Financial Code.

181 Subject to a few editorial changes.

182 European Commission, Proposal for a Directive of the European Parliament and of the Council on services in the internal market, (...), COM(2005) 603 final, Article 3(h).

of PSD2).[183] Such a service was not defined in PSD1 or in the European Commission's proposal for PSD2.[184] In its opinion, the ECB therefore recommended the addition of a definition encompassing "*providing authentication, authorisation, and other services related to the management of financial flows to the payee regardless of whether the payment service provider holds the funds on behalf of the payee;*"[185] and therefore excluding, in particular, authentification services from the scope of technical provision. The definition was partially incorporated in PSD2 without the clarifications provided by the ECB.[186] On the contrary, Recital 10 of the directive states that "*the mere processing and storage of data or the operation of terminals*" does not constitute the service of acquiring a payment transaction.

However, in order to benefit from this exclusion, it is no longer sufficient for a TSP simply not to come into possession of the PSU's funds. It must also not provide services that could be similar to, or participate in, payment initiation or account information, services that do not require coming into possession of the PSU 's funds.

Two cases are worth analysing.

(a) Companies managing digital portfolios

As mentioned above, major technology services companies such as Apple, Google, Samsung, etc., provide services that facilitate payments using mobile phones by digitising payment cards ("X-Pay" type services, such as Apple Pay, Google Pay, Samsung Pay, etc.), through digital wallets[187], the use of which has soared in recent

---

183 There is a significant shift in terminology between PSD1, which refers to the acquisition of a payment instrument, and PSD2, which refers to the acquisition of a payment transaction.

184 European Commission, "Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market, (...)", COM(2013) 547 final.

185 ECB, "*Opinion of the European Central Bank of 5 February 2014 on a proposal for a Directive of the European Parliament and of the Council on payment services in the internal market (...)*", (2014/C 224/01), Amendment 12, p. 11. The proposed definition was "*a payment service provided by a payment service provider contracting with a payee to accept and process the payee's payment transactions initiated by a payer's payment instrument, which result in a transfer of funds to the payee; the service could include providing authentication, authorisation, and other services related to the management of financial flows to the payee regardless of whether the payment service provider holds the funds on behalf of the payee;*".

186 Article 4(44) of PSD2: "*' acquiring of payment transactions' means a payment service by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of to the payee;*".

187 Or electronic wallets. All the terms digital wallets, e-wallets, digital portfolios and electronic wallets are considered equivalent.

years.[188] Digital wallets are used to make payments by payment cards (credit or debit), online and in shops. These digital wallets store virtual copies of payment cards and allow the cardholder to initiate a payment and make purchases using wireless technology for contactless payment by mobile phone (near field communication).[189] When users want to set up their digital wallet, they need to link their payment card to the wallet. This link involves creating a digitised version of the payment card (a token). However, most of the technology companies providing this e-wallet service do not have the appropriate authorisation[190] and consider that they benefit from the exemption relating to the provision of technical services.

As the European Commission points out, the suppliers of this type of "front end" technological solution, such as those of the "X-Pay" type for example, provide services that are very similar to payment initiation services, in that they effectively control the transaction initiation stage and the authentication of the PSU, whereas PSPs have limited control over the security and execution of these technical solutions,[191] even though, at the end of the chain, they are responsible for data security.[192] The difficulty is further exacerbated by the case law of the CJEU concerning the definition of a payment instrument, for which the technological function enabling contactless payment (near field communication or NFC), without having to make use of personalised security data, constitutes as such a payment instrument distinct from the payment card ("DenizBank" Ruling).[193] This interpretation of the CJUE is questionable as it broadens the definition of payment

---

188 The number of mobile wallets in use will reach 4.8 billion by 2025, compared with 2.8 billion in 2020. See Global Newswire, "*Study: More than half of the world's population will use mobile wallets by 2025*", 2021, available here.

189 S. Chaptal "*Apple Pay: NFC payment à la sauce Apple*", Revue Banque, September 2014, accessible here.

190 It should be noted that PayPal (Europe) S.à r.l. et Cie, S.C.A. has an entity authorised as a credit institution in Luxembourg and provides its electronic money and payment services from this entity (https://euclid.eba.europa.eu/register/cir/entityView/CRD_CRE_INS/549300ZV1RSA9F0LU821). This is not the case for Apple which, although it has an authorised vehicle in the EU, does not use it for the Apple Pay service.

191 DG FISMA, *op. cit.* p. 104.

192 See EBA, "*EBA clarifies the application of strong customer authentication requirements to digital wallet*", 31 January 2023: "*the Q&As, overall, clarify that issuers may outsource the provision and verification of the elements of SCA to a third party (e.g. by concluding contractual arrangements with the third party), such as a digital wallet provider, in compliance with the general requirements on outsourcing, including the requirements of the EBA Guidelines on Outsourcing arrangements . However, the responsibility for compliance with the SCA requirements cannot be outsourced and issuers remain fully responsible for the compliance with the requirements in PSD2 and the Regulatory Technical Standards (RTS) on SCA&CSC.*"

193 CJEU, *DenizBank AG v Verein für Konsumenteninformation*, Case C-287/19, 11 November 2020, recitals 79 and §2.

instruments given by the PSD2.[194] The CJEU dissociates contactless payment from the payment card and considers it to be a separate payment instrument. Indeed, it can be argued that it is simply a different means of communication between the terminal and the card, with the card linked to a single payment service user and the transactions charged to that user's bank account. Furthermore, the transaction is subject to the SCA obligation only above a certain amount, below which the transaction is exempt from such security. This interpretation has led to a lack of clarity and confusion among market participants.[195] In the light of this case law, the digital representation of the payment card, combined with the use of NFC technology, should logically correspond to the provision of payment services (in particular service No. 5 in Annex 1 of the PSD2, which consists of issuing payment instruments). This is in fact the opinion of the EBA, for whom the issuance of a token that is linked to an underlying payment instrument or the payment account of a payment service user constitutes in itself the issuance of a payment instrument and falls within the scope of the PSD2.[196] The question that arises is on whose behalf the token is created. If it is confirmed by the authorities or the courts that it is created on behalf of the issuing PSP, this could lead to the view that it is the issuing PSP that issues the payment instrument in this case. This raises the question of the role of "X-Pay" in relation to the issuing PSP. In contrast, the EBA specifies that other services provided by the digital wallet provider, such as the management of a digital wallet, do not fall within the scope of the directive due to their technical nature.[197]

A related issue is the legal liability associated with the implementation of strong authentication of the payment service user. Payment transactions carried out via a digital wallet also have an impact on the SCA. PSD2 requires PSPs to apply the SCA when the payment service user initiates electronic payment transactions.[198] The EBA has indicated that a PSP may use technology provided by a third-party provider (such as that used to unlock a mobile phone using facial or fingerprint recognition), while remaining responsible for security.[199] This refers to cases where mobile applications are installed on the phone and the PSP interacts with it for the purposes of the SCA. In this case, no contractual relationship is generally

---

194 Article 4(14) of the PSD2: " *a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order*".

195 DG FISMA, *op. cit.* p. 112.

196 EBA, "*EBA's response to the Call for advice on the review of PSD2...*", No. 85. See also DG FISMA, *op. cit.* p. 68, calling for a more holistic framework for providers of payment services.

197 *Ibid.*

198 Article 97(1) of the PSD2, transposed into Article L. 133-44 of the Financial Code.

199 EBA, Q&A 4047, available here.

established between the PSP and the smartphone manufacturer.[200] This poses difficulties, particularly when the PSP does not carry out any checks on security measures.[201] The EBA has clarified that the PSP may choose to outsource the customer's strong authentication to a technical service provider, provided that the PSP and the technical service provider enter into an outsourcing contract that complies with the rules on outsourcing critical or important functions governing such contracts. However, it has been observed that it is often difficult to set up such contracts, particularly with BigTechs, which consider that they are only making third-party technology available to the PSP. The PSD2 lacks details on the conclusion of these subcontracting agreements.[202]

(b) Other service providers whose services are similar to payment initiation

In the letter of the text, the payment initiation service is given a very broad definition in PSD2: "*a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider*".[203] The rules to be complied with for the provision of these services are also described very broadly in Article 66 of PSD2 and in the regulatory technical standards implementing PSD2. Whereas, in spirit, as reflected in the recitals of PSD2, these services appear to be more limited in scope: "*Those payment services play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account servicing payment service provider in order to initiate internet payments on the basis of a credit transfer*".[204]

There is therefore a discrepancy between the legislator's initial intention and the definition it finally adopted of the payment initiation service as well as the rules to be complied with to provide this service, which are broader in scope.

Furthermore, PSD2 only deals with payment initiation in a monolithic way, without considering the situation where several distinct players are involved at different stages of the payment initiation phase. This lack of precision raises questions in practice. For example, a company may, on a regular basis, entrust a service provider providing cash management services with the task of carrying out, in its name and on its behalf, certain operations relating to the management of its payment account

---

200 EBA, "*EBA's response to the Call for advice on the review of PSD2...",* no 313.

201 EBA, *op. cit*, no. 309 et seq.

202 EBA, *op. cit*, no. 315 et seq.

203 Article 4(15) of the PSD2, transposed into Article D. 314-2 of the Financial Code.

204 Recital 27 of PSD2.

opened with its PSP. In practice, this service provider is often not authorised to provide payment initiation services.

The type of operations carried out by such service providers varies according to the PSU and its needs: some service providers will only be involved in preparing the payment file (i.e., creating it based on instructions received from the PSP and formatting it), others will also be responsible for validating and/or sending the payment order to the PSP on behalf of the PSU. Still others may perform all these operations. The definition of the services performed and the role of these service providers is therefore open to debate, given the breadth of the text of PSD2 compared to its initial objective.

Two approaches can be adopted depending on whether the interpretation is made in the light of the recitals of PSD2 or in the light of the letter of the text of the directive.

In the absence of clarification, guidelines, doctrine or case law on the subject, it seems possible to interpret the definition of payment initiation in the light of the recitals of PSD2, which place it in the context of e-commerce. Recital 27 specifically targets "*those payment services [which] play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account servicing payment service provider in order to initiate internet payments on the basis of a credit transfer*".

A number of factors support this interpretation, including the report of the French National Assembly's Finance Committee on the draft law transposing PSD2 into French law, in which the payment initiation service is understood in the context of e-commerce: "*The first factor is the legal recognition at European level of two new types of player: payment initiation service providers and account information service providers. The former, also known as payment initiators, place payment orders at the consumer's request, from a payment account held with a bank. They enable consumers to pay for their online purchases simply by transferring funds, giving merchants the assurance that the payment has been initiated*".[205]

This interpretation is reinforced by the ACPR's description of payment initiation as "*[a] payment initiation service (defined in Annex I) which allows online merchants to accept credit transfers initiated on behalf of buyers*".[206] Lastly, it is consistent

[205] Report by the National Assembly on behalf of the Committee on Finance, the General Economy and Budgetary Control, on new reading, on the bill, amended by the Senate, ratifying Order No. 20171252 -of 9 August 2017 transposing Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (No. 812) dated 27 June 2018, available here.

[206] ACPR, "*Panorama des nouveaux acteurs de paiement*", March 2022, p. 13, available here.

with the legislator's objectives in creating the concept of payment initiation, such as the protection of payment service users' data and the development of e-commerce. Based on this interpretation, payment initiation refers only to transactions carried out in the context of e-commerce, so that the various situations described below do not fall within the scope of payment initiation services.

Nevertheless, the definition used in the PSD2 text and the rules laid down to govern this service are sufficiently broad to go beyond the scope of the services that the legislator wished to regulate, and encompass relations outside e-commerce. As a result, other use cases have developed, such as the case where a PSP offers a payment initiation service to multi-bank customers to enable them to manage their accounts. In view of the development of these multiple use cases, the qualification of the PISP has been questioned in certain cases.

In particular:

(i) Case 1: the TSP carries out each stage of the payment initiation process: preparing, validating and sending the order. The user only intervenes upstream to give instructions to the TSP. The TSP's involvement at the stage of sending the order would fall within the scope of payment initiation and this operating mode would therefore require the TSP to have authorisation.

By way of illustration, the user entrusts a service provider with all payroll management. At the user's request, the service provider prepares the files each month, validates them and sends them directly to the PSP account manager for payment of salaries on the correct date.

(ii) Case 2: the TSP prepares the payment file and sends the payment order to the PSP. The sending of the payment order by the TSP triggers the execution of the payment transaction by the ASPSP which holds the user's payment account, so that the TSP - and not the user - should be considered as having initiated the payment transaction. As a result, the TSP should have authorisation.

When it comes to accounting management or cash management outsourcing, there is software that can be used to forecast transactions to be carried out within a group of companies, in order to plan payments, for example, to suppliers. Based on an analysis of past transactions and information provided by the PSU, the service provider prepares files of future transactions. The payment service user validates the file and the service provider sends the payment order to the ASPSP. The service provider thus acts as a PISP.

(iii) Case 3: the TSP prepares, validates and sends payment orders for each user instruction. The part of this activity relating to sending the payment order is part of the payment initiation service and therefore also requires authorisation.

This is the case, for example, when employees request an advance directly on the TSP platform. When the employer agrees, the latter validates each request, one by one, and the TSP sends the payment order directly to the employer's PSP. The TSP thus acts as the PSP.

(iv) Case 4: the TSP's involvement is limited solely to preparing the payment file in the name and on behalf of the user, without sending the payment order. It should not fall within the scope of the PISP activity, including with regard to the text of PSD2.

In this context, there is uncertainty as to the regulatory consequences attached to the rights granted to the TSP by the payment service user. There appear to be two possible interpretations:

(A) granting a special mandate limiting the agent's powers only to transactions, in particular payment transactions, defined by the mandating user, and allowing the agent to access the account using his own identifiers would rule out classification as a PISIP. Thus, having his own access codes, there would no longer be any difficulties linked to web scrapping; or

(B) a mandate given to the service provider does not exempt it from PISP authorisation. A mandate does not exempt the service provider (agent) from the need to be authorised as a PISP, as long as the payments initiated in this way are made in the context of a regulated activity carried out on a professional basis. It is therefore perfectly possible to be both an agent and a PISP. The qualifications are cumulative. Supporters of this interpretation argue that since the PISP business is regulated, the exclusive nature of the mandate/PISP business would be tantamount to circumventing the obligations, particularly those relating to authorisation, whereas the entire business of certain service providers consists of managing and sending payment orders.

Although neither the PSD2, nor case law, nor doctrine provides any clarification on this subject, it could nevertheless be considered according to this interpretation that the sending of the payment order by the TSP to the ASPSP constitutes the triggering event for the payment transaction and that this action therefore falls within the scope of the payment initiation service. Consequently, the activity of a service provider

that merely sends the bank payment orders which were prepared and validated by the PSU itself would also fall under this classification.

This interpretation enables the ASPSP to detect in practice all cases where a third party is involved in initiating a payment, whether the user is a legal entity or a natural person, consumer or not, and thus avoids the practice of web scrapping. This is in line with one of the objectives of PSD2, which is to prevent the sharing of PSU identifiers with unregulated third parties and to limit the risks of fraud and data loss.

5.2.2. *Back-end service providers*

In addition, TSPs are also involved in "back-end" operations, to use the European Commission's terminology, i.e., providing a technical service enabling the PSP to provide payment services, without the TSP being visible to the payment service user or having any direct responsibility towards him, as it has no contractual link with him. In this case, the rules on subcontracting will apply, in particular those specific to PSD2.[207] In the field of information and communication technologies, the new European regulation on the digital operational resilience of the financial sector, also known as "DORA"[208], takes up these rules and refines them into a body of rules designed to provide a specific framework for "*financial entities' management of ICT* [information and communication technology] *third-party risk, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions*".[209] DORA thus brings TSPs within its scope by reiterating the fact that "*in light of the evolving payment services market becoming increasingly dependent on complex technical solutions, and in view of emerging types of payment services and payment-related solutions, participants in the payment services ecosystem, providing payment-processing activities, or operating payment infrastructures, should also be considered to be ICT third-party service providers under this Regulation, with the exception of central banks when operating payment or securities settlement systems, and public authorities when providing ICT related services in the context*

---

207 Article 19(6) of the PSD2. For a reminder of the legislation applicable to IT outsourcing in the banking sector, which also applies to the payments sector, see the HCJP report on the banking cloud: state of play and proposals, available here.

208 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

209 Recital 29 of DORA.

of fulfilling State functions."[210] As DORA points out, it would therefore be wise to align these two texts to ensure that they complement each other.[211]

5.2.3. *Special case of payment schemes*

The case of payment schemes such as Visa or Mastercard appears ambiguous. At first sight, they seem to be considered as communication services and therefore excluded from the scope of PSD2 by virtue of the exclusion of technical services.[212] In fact, some operators of these schemes are not authorised as PSPs within the EU.[213]

Visa and Mastercard are identified in the EEA as the two most important payment systems and are involved in facilitating communication between the acquiring institution and the issuing institution (see diagram below).[214]

---

210 Recital 63 of DORA.

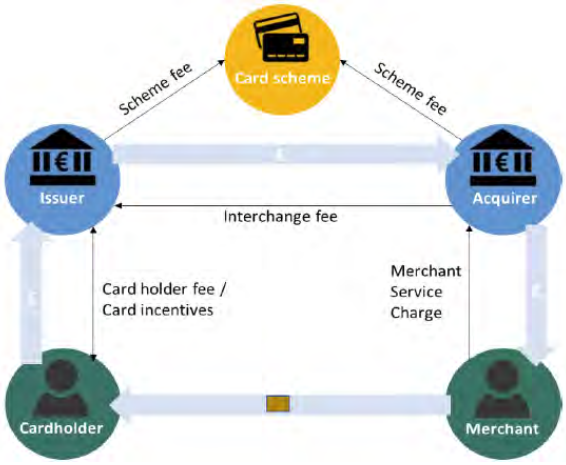
211 Recital 104 of DORA.

212 EBA, "*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*", EBA/Op/2022/06, 23 June 2022, no. 83: "*This is mainly due to the fact that they provide communication protocols used by PSPs for the application of SCA and other security requirements*".

213 Visa is a US payment scheme, which is operated in Europe by Visa Europe Limited (VEL), a UK-based company authorised as a payment institution by the FCA (authorisation available here), but which, since Brexit, no longer has regulated status in the EU. MasterCard is also an American payment scheme, which is operated in Europe by Mastercard Transaction Services (Europe), a Belgian company authorised as a payment institution in Belgium for services no. 3 and no. 4 of the PSD2, and is passported throughout the EU (https://euclid.eba.europa.eu/register/pir/view/PSD_PI/BE_NBB!0549987921).

214 DG FISMA, *op. cit.* p. 35.

Simplified diagram of a payment scheme[215]



For example, on the one hand, Mastercard indicates that it uses its central network to route a transaction to the issuer for approval. The aim is to simplify the exchange of information on transactions between issuers and acquirers and the settlement of the transaction by facilitating the exchange of funds between the parties via settlement banks chosen by them and their customers.[216] On the other hand, Visa says that in a typical Visa C2B payment transaction, where a consumer purchases goods or services from a merchant using a Visa card, the merchant presents the transaction data to an acquirer, typically a third-party bank or processor that accepts Visa cards or payment products, for verification and processing. Through VisaNet, the acquirer presents the transaction data to Visa who, in turn, contacts the issuer to verify the account or credit line of the account holder for authorisation. Once the transaction is authorised, the issuer actually pays the acquirer an amount equal to the value of the transaction, less the interchange reimbursement fee, and then posts the transaction to the consumer's account.[217]

However, the services provided by payment schemes are not limited to the provision of communication networks and include payment services. Visa, for example, operates a cross-border transfer service called Visa B2B Connect,[218] based on the tokenisation of participants' sensitive banking information (account numbers) by giving them a unique identifier that can be used to facilitate transactions across the network. The ACPR has also noted the increasing "*dependence of the entire payment chain on international card schemes*" linked to

215 DG FISMA, *op. cit.* p. 36.

216 Mastercard Inc. annual report, 2021, pp. 9-10, available here.

217 Visa Annual Report 2022, p. 5, available here.

218 https://www.businesswire.com/news/home/20190611005296/en/.

"*the growth in the use of tokenisation* ".[219]In this case, the exception relating to the provision of technical services is no longer sufficient.

It should be noted that PSD2 provides for another exception, relating to "*payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers,* (...);".[220] A payment system is also defined as "*a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions*"[221]. The question arises as to whether this notion of payment system is limited to systems notified to the European Commission in application of the Finality Directive[222] (which would have the effect of excluding payment schemes such as Visa), or whether it encompasses any system that meets the functional definition provided by PSD2. It is this second meaning that is relevant. Indeed, PSD2 specifically refers in its recitals to card schemes involving four parties, as well as the main systems for processing credit transfers and direct debits.[223] In practice, this means that it targets payment schemes, which may be domestic, such as *GIE Cartes Bancaires* in France, or international, such as Visa and Mastercard.[224]

However, even if they are excluded from the scope of application of PSD2,[225] certain payment systems or schemes, particularly systemic ones, are covered by the Eurosystem's supervisory framework for electronic payment instruments, systems and devices ("**PISA**")[226]. That said, submission to the PISA supervisory framework

---

219 Report, ACPR, "*La surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers*", 2020, available here.

220 Article 3(h) of the PSD2. It should be noted that this exclusion has not been transposed into French law, which creates some legal uncertainty when the payment system or scheme provides payment services on French territory.

221 Article 4(7) of the PSD2.

222 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems.

223 Recital 49 of PSD2.

224 It should be noted that, in its opinion on the PSD1 proposal of 26 April 2006 (ECB/2006/21), the ECB even recommended that the definition of payment system should include an express reference to systems covered by the purpose directive (Modification no. 7, p. 22).

225 Subject, however, to MasterCard, which is approved as a payment institution.

226 Eurosystem Oversight Framework for Electronic Payment Instruments, Systems and Devices ("PISA Framework"), November 2021, accessible here. *Payment schemes* that are supervised by the ECB under the PISA Framework include, among others, MasterCard Europe and Visa Europe, the list can be accessed here. See also, Regulation (EU) No 795/2014 of the European Central Bank of 3 July 2014 on oversight requirements for systemically important payment

applies equally to players authorised as payment institutions[227] , and those not authorised under PSD2[228]. Submission alone should therefore not be a reason for excluding payment schemes *ipso facto* from the scope of PSD2.

Despite this, the EBA notes that card payment systems play a crucial role in ensuring that PSPs participating in the systems comply with certain legal requirements arising from PSD2, such as strong customer authentication (SCA), because of the communication protocols they provide and which are used by PSPs to implement these requirements.[229] In fact, the "3D secure" protocol, which is a system for securing online payments originally created by Visa and Mastercard, has become the standard for authenticating card payments, which raises questions not only in terms of a de facto monopoly in a theoretical sector of activity for the payment services union, but also in terms of European sovereignty, given the nationality of these two players.

Ultimately, it would be necessary to clarify the relationship between PSD2 and the ECB's framework for supervising payment systems, by specifying that the exclusion contained in PSD2 applies only to systems subject to the Finality Directive and to those not subject to it but supervised by the ECB, so that only a system supervised under EU law benefits from the exclusion. Incidentally, the question may be raised as to whether it would not also be necessary to specify, in the payment system definition provided for in PSD2, that the operator of the system, the concept of which should be clarified, should have its registered office in the European Union.

5.3. **HCJP recommendations**

The HCJP proposes the following recommendations:

> **Recommendation No. 9**: The HCJP recommends clarifying the concepts of "initiation of a payment transaction" and "payment instrument", with a view to specifying the conditions under which: (i) in the case of card payments; and (ii) more generally, the technological solutions provided by

systems (ECB/2014/28), accessible here. *Adde*, ECB, "*Oversight framework for card payment schemes - standards*", January 2008, accessible here.

227 Such as Mastercard, which has a payment institution authorisation in Belgium.

228 Such as Visa Europe (*c.f.*, list of schemes in the PISA monitoring framework maintained by the ECB, accessible here).

229 EBA, "*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*", EBA/Op/2022/06, 23 June 2022, No. 83.

technical service providers can be distinguished from the payment services provided by PSPs.

Recommendation No. 10: The HCJP recommends clarifying the regulatory framework applicable to subcontracting to TSPs, particularly between DORA and the PSD.

Recommendation No. 11: The HCJP recommends clarifying the definition of payment system or scheme, so as to link the corresponding exclusion to the submission of the payment system or scheme to the Union's Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA).

6. EXCLUSIONS FROM THE SCOPE OF THE PSD - INTRA-GROUP EXCLUSION

6.1 Issues linked to intra-group exclusion

Cash pooling[230] is common practice within groups of companies, particularly international groups. It can take several forms: either it is based on actual cash movements between the companies in the group, with one of them acting as the centralising agent - usually referred to as the "pivot" company (this form corresponds to "real" centralisation of financial flows); or it is based on merging the scales of interest owed by the companies in the group into a cash pooling account held by the pivot company (this is known as "notional" centralisation).[231] In France, cash pooling is not covered by a specific legal framework. However, as it generally involves the performance of certain banking transactions subject to the banking monopoly, both in respect of credit transactions carried out on a regular basis and the receipt of repayable funds from the public,[232] it is subject to dedicated provisions providing for exceptions to this monopoly.[233]

However, cash pooling does not only involve carrying out banking transactions.[234] It also involves carrying out payment transactions, which entails the provision of payment services within the meaning of the PSD. The introduction of a single European market for euro payments (SEPA zone) has opened up new opportunities for cash pooling within groups of companies. In this context, the pivot company is responsible for centralising payments on behalf of all the companies in the group that are members of the cash pool (in practice, the term "payment factory" is often used). This centralisation of payments works in both directions: the central company can make payments to third parties on behalf of a group company (payment qualified as a POBO (payment on behalf of)) or receive from a third party a payment due to another group company (payment qualified as a ROBO or COBO (reception or collection on behalf of)).

---

230 Also known as " cash omnium", etc.

231 See for a more detailed description: Banque de France, "*Le cash pooling*", V15/11/2016, accessible here.

232 Respectively, articles L. 311-1 and L. 511-5 of the Financial Code.

233 Articles L. 312-2, §1° and L. 511-7, §3° of the Financial Code.

234 According to the current understanding of this concept, resulting from the transposition of the PSD1. Since then, banking operations have included only payment banking services, alongside the receipt of funds repayable from the public and credit operations.

6.2. What is the current legal regime?

6.2.1 *In PSD2 (and other relevant European legislation)*

In France, prior to the transposition of PSD1, the current payment services were contained within the concept of management of means of payment, which came under the banking monopoly. Consequently, the aforementioned exceptions applicable to banking services were sufficient to cover all banking transactions (including, therefore, payment services) carried out as part of cash pooling within a group of companies.[235] By separating payment services from banking services (and therefore from the related monopoly), PSD1 has changed the situation, so that a specific exception to the PSP monopoly has been made necessary.

The PSD1 therefore offered EU Member States the possibility of excluding from the scope of the payment services regime payment transactions "*between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group*" (Intra-group Exclusion). Thus, in Member States that have transposed the Intra-group Exclusion, the rules applicable to payment services provided in that Member State do not apply to payment transactions carried out between entities in the same group (*e.g.*, it is not necessary to have a minimum payment institution license to provide the said services). Article 3(n) of PSD2 incorporates this exclusion without change.

However, it should be noted that the Intra-group Exclusion only covers payment transactions within the group of companies, but not the provision of payment services. This is an important distinction, because while payment services provided by one group company to another in connection with such transactions are necessarily covered by this exclusion, the same does not apply to payment services provided in connection with payment transactions carried out outside the group, i.e., to or from third parties (in other words, POBO and ROBO payments). In particular, it should be recalled that the activity of collecting funds on behalf of third parties involves the provision of payment services, according to the EBA and, in France, the ACPR.[236]

For this reason, recital 17 of PSD2 specifies that Intra-group Exclusion may apply to the centralisation of payment orders on behalf of a group by a parent undertaking or its subsidiary: "*The Single Euro Payments Area (SEPA) has facilitated the creation of Union wide -'payment factories' and 'collection factories', allowing for*

---

235 See above, footnote no. 233.

236 See section 4 (*Material scope of PSD2 - Collection of funds on behalf of third parties*) of this report.

the centralisation of payment transactions of the same group. In that respect payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking provided by a payment service provider belonging to the same group should be excluded from the scope of this Directive. The collection of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission to a payment service provider should not be considered to be a payment service for the purposes of this Directive".

However, this approach of clarifying the substance of the text of the directive by means of a recital poses two difficulties. The first is methodological. This clarification only serves as a rule of interpretation and does not appear in the text of the Intra-group Exclusion itself. When a directive is transposed, its recitals are very rarely transposed and the result is uncertainty as to their scope when, having not been transposed, they are invoked before the courts or supervisory authorities. Moreover, we shall see that the approaches adopted by certain Member States, as to whether or not to transpose recital 17 or to give it normative scope, are variable,[237] which undermines the consistency of the texts transposing the directive within the Union and creates real difficulties for groups of companies that have set up pan-European cash pooling.

The second concerns the very substance of the interpretation contained in this recital. While the recital refers to "*the creation of Union wide -'payment factories' and 'collection factories'*[238]*, allowing for the centralisation of payment transactions of the same group*", which includes both POBO and ROBO payments, the conclusion of the recital is more ambiguous as to whether POBO and ROBO payments are excluded from the scope of the directive: "*The collection of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission to a payment service provider should not be considered to be a payment service for the purposes of this Directive*". A literal reading of this sentence suggests that ROBO payments fall outside the scope of the Intra-group Exclusion.

This raises the question of the exact scope of this exclusion.

6.2.2. *In Member States' legislation*

In France, the Intra-group Exclusion has been transposed by reproducing *verbatim* Article 3(n) of DPS2, but adding the clarification provided by Recital 17: "*Is not considered to be a payment service (...) 4° The execution of payment transactions between a parent undertaking and its subsidiary, or between subsidiaries of the same parent undertaking, or within a group within the meaning of Article L. 133-*

237 See paragraph 6.2.2of this report.

238 Underlining added.

4, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group, and the collection of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission to a payment service provider"[239].However, within the European Union, the Intra-group Exclusion has not been transposed in a uniform manner.

This is the case, for example, in Italy, which has transposed the Intra-group Exclusion to include the centralisation of payment orders[240] , and - to a lesser extent - in Germany. Although German law specifies that the Intra-group Exclusion does not apply when a group entity makes or receives payments for the benefit of an entity outside the group, there is a practice of exclusion agreed between the BaFin and the Association of German Treasurers under which entities in the same group are only authorised to carry out cash movements (*e.g.*, cash pooling) if all the entities are subject to the same risk management rules.[241]

On the other hand, in Spain, Luxembourg and Poland, the Intra-group Exclusion has been transposed using only the narrow wording of Article 3(n) of the PSD2, without including Recital 17 of the PSD2: centralisation of payment orders is therefore not included *a priori* in the scope of the Intra-group Exclusion.

6.3. **HCJP recommendations**

The centralisation of payment orders and payments *via* a central treasury (both POBO and ROBO payments) is not only a widespread practice among groups of companies, but also one that is not confined to the borders of a single Member State. However, differences in transposition within the EU and legal uncertainty as to the scope of recital 17 of the PSD2 (transposed or not) affect legal certainty. In order to reduce this uncertainty, it would be advisable to specify unambiguously that the Intra-group Exclusion applies to the centralisation of payments received, as well as for the benefit of third parties, on behalf of entities belonging to the same group, in order to harmonise the legislation of the Member States.

> **Recommendation No. 12:** The HCJP recommends amending the PSD2 to specify in the text of the Intragroup Exclusion that this exclusion applies to the centralisation of payments received from third parties as well as to the benefit of third parties, on behalf of entities belonging to the same group.

239 Article L. 314-1 III 4° of the Financial Code.

240 Article 2(2)(p) of Decree no. 11/2010.

241 BaFin website, accessible here.

7. NOTION OF PAYMENT ACCOUNT

7.1. Issues relating to the definition of the payment account

One of the innovations of PSD1 was the creation of the concept of "payment accounts", which has been incorporated unchanged into PSD2. A payment account is defined as "*account held in the name of one or more payment service users which is used for the execution of payment transactions*".[242] The payment account is characterised by its purpose: that of executing any "*act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee*",[243] i.e., for example, the withdrawal or payment of cash, credit transfers, direct debits, etc., for the purpose of making a payment.

Since PSD1, the payment account has become an essential concept used by a number of European texts, particularly Level 1 texts: Regulation (EU) 260/2012, defining the technical standards applicable to credit transfer and direct debit transactions in euros (SEPA Regulation) and Directive 2014/92/EU, on payment accounts (PAD Directive), Regulation (EU) 2015/751, on interchange fees for payments based on a payment card (Interchange Regulation), Regulation (EU) 2015/847, on information accompanying transfers of funds and Regulation (EU) 2021/1230, on cross-border payments. There is also the EMD2.

However, the concept of a payment account is not essential to PSD2. In fact, the directive aims to regulate the provision of payment services in the EU by payment service providers.[244] Moreover, it should be noted that maintaining a payment account does not in itself constitute a payment service.[245]

---

242 Article 4(12) of PSD2 (formerly article 4(14) of PSD1). Transposed into article L. 314-1-I of the Financial Code.

243 Article 4(5) of PSD2, transposed into Article L. 133-1-I of the Financial Code. See G. Goffinet, "*Le régime des comptes de paiement vu par le régulateur*", Banque & Droit, Nov.-Dec. 2016, special issue "*Nouveaux comptes et intérêts négatifs*", p. 21. See also L. de Pellegars, "*Le compte de paiement*", Banque & Droit no. 134, Nov.-Dec. 2010, p. 14; D. Stucki and N. Kanhonou, "*Le compte de paiement: une notion juridique stable pour une utilisation évolutive*", Banque & Droit, hors-série, November-December 2019, p. 18; P. Storrer, "*Brêves remarques sur le compte de paiement*", Revue Banque no. 788, 13 October 2015.

244 Articles 1 and 2 of the PSD2.

245 See the list of payment services in Annex 1 of PSD2.

That said, as the European Commission[246] and the EBA point out,[247] the concept of payment accounts is controversial.

Firs, because, in terms of European legislation, PSD2 does not have a monopoly on its definition. In fact, since PSD1, other legislative texts have defined payment accounts independently for the purposes of their respective application. In fact, there is no single definition of payment accounts, which may seem paradoxical given that this is an important concept in the regulation of payment services in the broad sense, and moreover, it is contained in a single directive while European regulations (such as SEPA Regulation and Interchange Regulation), directly applicable in the Member States, refer to this concept.[248]

It should be noted in particular that the SEPA Regulation[249] links the IBAN number[250] inseparably to a payment account.[251] In other words, for the purposes of executing a payment transaction consisting of a credit transfer or a direct debit,[252] any payment account must have an IBAN number. Consequently, while any payment account falling within the scope of the SEPA Regulation[253] must have an IBAN number, the reverse does not seem to be true. In fact, an account with an IBAN number is not necessarily a payment account, as such a number can be assigned to any type of account.

---

246 DG FISMA, *op. cit*, spec. § 5.1.4, p. 111: "*Surely the most controversial across all stakeholders is the definition of "payment accounts": this is a key definition [...]*".

247 EBA, "*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*", EBA/Op/2022/06, 23 June 2022.

248 On the proposal to transform PSD2 into a European regulation, see section 1 (*Replacing the Directive with a Regulation*) of this report.

249 Which lays down the rules for credit transfers and direct debits denominated in euros within the EU when both the payer's and the payee's payment service providers, or the sole payment service provider involved in the payment transaction, are located in the EU.

250 International bank account number, defined as "*an international payment account number identifier, which unambiguously identifies an individual payment account in a Member State, the elements of which are specified by the International Organisation for Standardisation (ISO)*" (Article 2(15) of the SEPA Regulation). The IBAN is a kind of number plate for a bank account, enabling it to be identified. It consists of a variety of alphanumeric characters with a minimum of 14 but can be up to 34 characters long. The length of the IBAN depends on the country. In France, IBAN codes are 27 characters long. The first two characters represent the code of the country of origin (for example, FR for France). See the ISO website: https://www.iso.org/obp/ui/#iso:std:iso:13616:-1:ed-2:v1:en.

251 Article 5(1)(a) of the SEPA Regulation, referring to paragraph 1(a) of its Annex.

252 Provided that the PSP of the payer and that of the payee (or the sole PSP involved in the payment transaction) are located in the EU.

253 See in particular the exceptions provided for in Article 1(2) of the SEPA Regulation.

Secondly, because by creating the payment account and submitting it to autonomous regulation, distinct from that which generally applied to the banking sector[254], the PSD has given rise to a boundary conflict with pre-existing related concepts, such as "bank" accounts[255], or new accounts, such as the "specific" e-money account referred to in the EMD2.[256] Finally, given the freedom of interpretation afforded by the absence of a single precise conceptual definition, it is sometimes difficult to distinguish a technical (or accounting) account from a payment account.

7.1.1. *Deposit and payment accounts*

First of all, as far as deposit accounts are concerned, it is important to understand how a payment account differs from a deposit account.

Unlike payment accounts, deposit accounts are not defined by law (either in European legislation or in French law). Moreover, the concept of deposit account is sufficiently broad to encompass different types of account, which moreover have no official or regulated meaning that would characterise them in a general way. There are deposit accounts in the *stricto sensu* (often referred to in practice as current accounts), cheque accounts, demand deposit accounts etc.[257] These accounts are generally used in day-to-day life, for domiciling income, paying day-to-day expenses etc. These accounts generally have associated means of payment, such as payment cards and cheque books.[258] They are distinct from savings accounts, which, under different names,[259] are not generally used for day-to-day spending and are only funded from the holder's current account (or debited to that

---

254 Cf. article L. 311-1 of the Financial Code prior to PSD1: the management of means of payment came under the banking monopoly.

255 More specifically, a deposit account. The term bank account, which has a long and familiar history, does not correspond to a precise legal reality. Consequently, the more precise term deposit account is preferred.

256 See paragraph 7.1.2 of this report.

257 However, see CNC Decision 69-02 of 8 May 1969 on the conditions for the receipt of funds by banks (the "**1969 CNC Decision**"), which distinguishes between a first category, sight accounts, and a second category, passbook or term accounts. This decision adopts a negative concept of the sight account. A sight account is therefore an account that does not meet the conditions applicable to the second category of accounts.

258 We can already see the *hiatus* between two distinct legal regimes: while the issuing of a payment (or credit) card is in fact a payment service subject to PSD2 (service no. 5, Annex 1, PSD2), the issuing (and cashing) of cheques is excluded from its scope (article 3(g) of PSD2), and falls, in France, under payment banking services (article L. 311-1 of the Financial Code), which are covered by the banking monopoly (article L. 511-5, para. 2 of the Financial Code).

259 In France, passbook accounts (unregulated), regulated savings accounts (*Livret A, Livret de Développement Durable et Solidaires* (LDDS), etc.).

account), originally within the same bank[260], although this will no longer be the case from the end of 2022.[261] That said, this is not an absolute distinction, since a savings account can also be used for day-to-day spending, allowing payment transactions to be debited from it.[262] Finally, what all so-called "bank" accounts have in common is that the bank receives deposits or other repayable funds from its customers. These concepts are not defined in European legislation either.[263] The ECJ considers that the repayable nature, whether intrinsic or not, is an essential characteristic of a deposit.[264] The right of use granted to the credit institution receiving them is a truly distinctive criterion, which is specified in French law.[265]

Therefore, according to the literal definition of a payment account contained in the PSD2, a deposit account which allows payment transactions to be debited or credited to it should necessarily be a payment account and the credit institution holding the account a PSP within the meaning of the PSD2.[266] However, the opposite is not true for a payment account held by a payment institution. In fact, by removing the provision of payment services from the scope of the banking monopoly on the receipt of deposits[267] through the creation of a new category of

---

260 In France, see the CNC Decision of 1969: concerning passbook accounts: "Transactions recorded on passbook accounts are limited to deposits or withdrawals in favour of the holder or to transfers from or to his current account" (article 2(B)(2)), and term accounts: "A separate account must be opened for each time deposit transaction; each of these accounts may only record the transfer or payment entry for the funds to be blocked, the account closing entries and the entry for the account balance on the due date" (article 2(C)(2)).

261 Decree of 10 November 2022 amending the CNC Decision of 1969, which now allows transfers between accounts belonging to the same holder at different institutions.

262 In France, see article R. 221-5-II of the Financial Code concerning the *Livret A*. However, as the *Livret A* is not considered to be a payment account within the meaning of PSD2, because its purpose is savings and not to carry out payment transactions (G. Richard, "*Nouveau d'accès aux comptes et aux données des comptes*", Banque & Droit, hors série, March 2019, p. 15; P. Storrer, "*Brèves remarques sur le compte de paiement*", Revue Banque no. 788, 13 October 2015 .).

263 Article 9 of the CRD, which is the seat of the monopoly on the receipt of deposits or other repayable funds from the public, does not define any of these concepts. Paragraph (14) of the preamble to the CRD merely states that the receipt of repayable funds from the public may take forms such as the continuous issue of bonds or other comparable securities. There are no definitions of these concepts in the CRR Regulation either.

264 See ECJ, Case C-366/97, *Romanelli*, 11 February 1999. Also article L. 312-2 of the Financial Code.

265 Article L. 312-2 of the Financial Code: "*Funds that a person receives from a third party, in particular in the form of deposits, with the right to dispose of them on his own account but with the obligation to return them, are considered to be funds repayable from the public*".

266 See articles 1(a) and 4(11) of the PSD2.

267 Set out in Article 9(1) of the CRD, transposed into Article L. 511-5, paragraph 1er of the Financial Code.

players, payment institutions,[268] the European legislator correlatively prohibits payment institutions from receiving deposits or other repayable funds from the public, in a similar way to electronic money institutions.[269] That said, the boundary may sometimes seem tenuous on the surface: when the institution receives funds from users with a view to carrying out future transactions,[270] does the payment institution not receive a form of deposit, all the more so if, as PSD2 authorises, the funds are protected by an insurance policy or a guarantee, rather than by ring-fencing?[271] In reality, the fact remains that the PI cannot use the funds received from payment service users for any purpose other than the provision of payment services, because it simply cannot dispose of them for its own account.[272]

However, can it be said, as stated above, that a deposit account is necessarily a payment account? Is the finalist definition sufficient to distinguish them when the deposit account does not have the functionalities of a payment account? This very question has arisen in connection with savings accounts, which, when intended solely for savings purposes, should not be classified as payment accounts. However, it can only be accepted that at least two payment transactions are carried out, on the one hand to the credit of the account, when the holder tops it up, and on the other hand to the debit of the account, when the same holder withdraws his savings from the account.[273] However, it should be noted that these transactions often involve the same person as payer and beneficiary, *i.e.*, the holder, who uses two accounts belonging to him: his deposit account - or payment account, as it should be called - and his savings account. In the absence of the PSD2, the PAD Directive excludes them from its scope (which is admittedly narrower than that of the PSD2).[274] This

---

268 Paragraph (10) of the preamble to the PSD1.

269 Article 18(3) and (5) of the PSD1. If the institution has not opted for an insurance policy or a guarantee, this also means that it must keep these funds in a separate account with a credit institution or invest them in low-risk, liquid and secure assets (Article 10(1)).

270 Article 10(2) of the PSD2 (and, in France, article L.522-17-II of the Financial Code).

271 Article 10(1)(b) of the PSD2.

272 See paragraph (34) of the preamble to PSD2, in connection with article L. 312-2 of the Financial Code mentioned above.

273 This demonstrates the provision of services 1, 2 and 3(c) of Annex 1 of PSD2 by the account-holding bank.

274 Paragraph (12) of the preamble to the PAD, unless they "*used for day-to-day payment transactions and [were to] comprise all of the functions listed above*" attributed to the payment account by the PSD2. See *below*, the ING DiBA ruling in paragraph 7.7.2.7.2.2 of this report.

approach is generally accepted in the literature,[275] although it is debatable given that a savings account can be used to carry out payment transactions.[276]

7.1.2. *Specific electronic money account and payment account*

Secondly, the EMD2 incidentally created the concept of an electronic money account, merely stating that "*the definition of electronic money should cover electronic money whether it is held on a payment device in the electronic money holder's possession or stored remotely at a server and managed by the electronic money holder through a specific account for electronic money*",[277] without defining it[278] but recognising that this *sui generis* account has the capacity to store electronic money. It follows from the definition of electronic money that it can be issued on different media, *i.e.*, either on a physical medium capable of possession (such as a card), or on a software medium (in which computer accounts are created) in which the units of electronic money are recorded. In reality, it does not matter in practice, because if the electronic money is not stored in a payment card, the user opens an account with the electronic money issuer in order to be credited with the electronic money issued by the issuer,[279] , which is frequently referred to in practice as a *wallet* or *e-wallet*, an account to which payment instruments such as payment cards may be associated without the latter directly storing the electronic money.[280]

Although, from a legal point of view, this account cannot be confused with a deposit account, in the same way that a payment account held by a payment institution

---

275 Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), Rapport, "*Analyse nationale des risques de blanchiment de capitaux et du terrorisme en France*", January 2023, spec. p. 79: "*The payment account is defined in I of Article L. 314-1 of the Monetary and Financial Code and allows deposits, but not all deposit accounts are payment accounts (e.g. savings accounts)*"; G. Richard, "Nouveau d'accès aux comptes et aux données des comptes", Banque & Droit, hors-série, March 2019, p. 15; P. Storrer, "*Brèves remarques sur le compte de paiement*", Revue Banque, No. 788, 13 October 2015.

276 See footnote no. 262 above.

277 Recital 8 of EMD2. This concept did not exist under EMD1.

278 In fact, the Banque de France prefers to refer to electronic money wallets (https://particuliers.banque-france.fr/info-banque-assurance/compte/les-differents-types-de-comptes).

279 See PayPal's terms and conditions, available here. https://www.paypalobjects.com/ua/FR_fr_FR/ua.pdfNote that this is a credit institution. The account is sometimes also referred to as a *wallet*. See Lydia's terms and conditions, available here.

280 EBA, "*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*", EBA/Op/2022/06, 23 June 2022

cannot serve as a receptacle for public deposits,[281] the balance of this electronic money account does constitute a claim for repayment against the electronic money institution,[282] which brings it closer to scriptural money - *i.e.*, the balance of a deposit account.[283] Moreover, the electronic money account fulfils the same functions, beyond simply storing monetary value in electronic form, *i.e.*, to enable payment transactions to be carried out, *i.e.*, in particular, to transfer the claim to the balance of the account belonging to the holder (payer) to another person (payee).[284] However, the procedures for transfers between electronic money accounts and payment accounts are legally different, particularly when the transfers fall within the scope of the SEPA Regulation.

On the other hand, it is questionable whether it constitutes a payment account.[285] Indeed, the EMD2 maintains the ambiguity when it states that the definition of electronic money "*should cover all situations where the payment service provider issues a pre-paid stored value in exchange for funds, which can be used for payment purposes because it is accepted by third persons as a payment*". Moreover, the PSD2 itself provides that electronic money may be stored on a payment account.[286] For its part, recital 12 of the PAD Directive excludes, as a rebuttable argument, electronic money accounts from the scope of payment accounts because of the generally more limited functionalities of such accounts. Finally, doesn't the Interchange Regulation also specify that a payment account is "*an account held in the name of one or more payment service users which is used for the execution of payment transactions, including through a specific account for electronic money as defined in point 2 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council*"?[287] The dividing line between the means of payment constituted

---

281 Article 6(2) and (3) of the EMD2.

282 Article 2(2) of EMD2: electronic money is "*electronically, including magnetically, stored monetary value as represented by a claim on the issuer*".

283 However, it cannot be a means of saving (recital 13 of the EMD2). However, it should be noted that the parallel is limited by the fact that, whereas a deposit account gives rise to a claim by the account holder against the account keeper (and not against the issuer of the currency itself), electronic money gives rise to a claim against the issuer of the electronic money alone.

284 See for example article 4.2 (Account operation) of the Mangopay general terms and conditions; article 3 (Sending money) of the PayPal general terms and conditions.

285 See M. Roussille, "*La notion de compte de paiement*", Banque et droit, nov.-déc. 2016, hors-série "*Nouveaux comptes et intérêts négatifs*", p. 12. Spec: "(...) *is the e-money account in principle a payment account, since its purpose is to enable its holder to receive e-money units or to pay creditors in e-money units. The concept of a payment account thus reflects the fact that it is subject to a regime that is cumulative with the specific rules applicable to each type of account*".

286 Article 63(3) of the PSD2.

287 Article 2(22) of the Interchange Regulation, defining the payment account. See also, P. Storrer, "*Brèves remarques sur le compte de paiement*", Revue Banque, No. 788, 13 October 2015.

by electronic money and the payment instruments used to transfer funds from, or to, the payment account therefore becomes very thin, all the more so when the payment account can be credited with sums intended for the execution of future payment transactions.[288] Finally, as one author noted in 2010, "*the difference between an e-money account and a payment account will become very tenuous if we consider the parallel development of dematerialised means of payment backed by payment accounts (transmission of orders by mobile phone, etc.). Indeed, how can we distinguish between the holder of a payment account who transmits an order using a virtual card attached to a payment account and the holder who issues an order using an electronic money account number*?[289] Thirteen years later, DG FISMA is saying the same thing.[290] According to the e-money operating models, certain e-money accounts could be qualified as payment accounts when their functionalities are significant and comparable to a payment account.

7.1.3. *Technical account and payment account*

The concept of a "technical" account is even more difficult to grasp, as it covers very different realities, depending on the objectives that this type of account seeks to pursue.[291] Moreover, it should not be misunderstood: in double-entry bookkeeping, all debts and receivables give rise to debit and credit entries in accounting accounts (particularly third-party accounts: customers, suppliers, creditors of all types, etc.).[292] Do these accounts necessarily have to be classified as payment accounts?

Since factual situations are specific, a case-by-case analysis, based on a few examples, is necessary.

A first example can be drawn from the fact that, for some years now, major international banks have been offering their customers, often large industrial groups, the possibility of opening technical or administrative accounts, known as "virtual" accounts, designed to facilitate their cash management.[293] In practical terms, a bank holding a company's payment account (known as a master account or

---

288 See *supra* note no. 270.

289 L. de Pellegars, "*Le compte de paiement*", *op. cit.* p. 16.

290 DG FISMA, *op. cit.* p. 40.

291 In practice, these accounts are often referred to as virtual accounts, suspense accounts, intermediary accounts and so on.

292 ANC Regulation No. 2014-03 of 5 June 2014 on the general chart of accounts. Class 4 accounts (third party accounts).

293 See for example: Oracle, "*Virtual accounts*", white paper, November 2018, accessible here, BNP Paribas, accessible here, JPMorgan, accessible here, Deutsche Bank, accessible here, Goldman Sachs, accessible here, etc.

sometimes a physical account) offers its customers the option of opening so-called virtual accounts for the company's subsidiaries. Each subsidiary has its own virtual account. The purpose of these accounts is to record debit and credit transactions corresponding to payments made or received by the company from the master account, acting in the name and on behalf of its subsidiaries.[294] IBAN references may be associated with these accounts.[295] The question has arisen as to whether these virtual accounts constitute payment accounts subject to the provisions of PSD2, particularly in the context where such accounts are allocated an IBAN reference (also described as virtual) and that, in certain cases, the subsidiaries to which these accounts are allocated may notify payment orders to the bank holding the master account on behalf of the company that holds it.

If we adhere to the finalist definition of a payment account,[296] then, in this context, these virtual accounts should not be qualified as such. In fact, the sole purpose of these accounts is the administrative and accounting monitoring of payments received or made on behalf of subsidiaries as part of the management of flows within the payment factory of the group of companies concerned, and payment transactions are only carried out to the credit or debit of the master account, the entries made in the virtual accounts merely reflecting this.[297]

A second example can be drawn from the model of PIs and EMEs that mandate agents, such as marketplaces. In this model, the funds of payment service users (generally legal entities) are collected on a single account opened in the name of the agent (also known as a "master account"). Payment cards belonging to the users are indirectly attached to this account. More precisely, between the "master account" and the payment cards there are "technical" accounts, opened in the name of the holder of each payment card. These accounts, which have a zero balance, are mainly used to segregate payment flows by cardholder. However, funds do pass

---

294 POBO (payment of behalf of) and ROBO (receipt on behalf of) payments. The advantage of these accounts is that they eliminate the need to open as many physical accounts as there are subsidiaries, or even for each business unit within a subsidiary or, in a matrix approach, within a particular geography (see e.g. Goldman Sachs and Deloitte, "*Virtual Account Management: A foundational imperative for cash concentration*", 2020, p. 2).

295 See above, note no. 250. It is a technical standard and is therefore not legally binding. However, this standard is used by the SEPA Regulation, which defines it as "*an international payment account number identifier, which unambiguously identifies an individual payment account in a Member State, the elements of which are specified by the International Organisation for Standardisation (ISO)*" (Article 2(15) of the SEPA Regulation) and makes it mandatory for payment accounts concerning credit transfers and direct debits (Article 5(a) of the SEPA Regulation).

296 Particularly in the light of the ING DiBa ruling (see paragraph 7.2.2 of this report).

297 Payment transactions cannot be made directly from virtual accounts and an intermediary account (the master account) must be used. This corresponds to the situation described in the ING DiBa judgment (see recitals 32 and 33 of the decision).

through these accounts, because when a card payment transaction is made, the amount of the purchase is debited from the "master account", credited to the "technical" or transit account, and ultimately transferred to the PI or EME settlement account for transmission to the card payment system. According to the ACPR, the recording of incoming and outgoing flows to and from this account and the execution of the card payment transaction from this account enable it to be classified as a payment account.

A third example is the outsourcing of the card issuing service by one PSP to another PSP, a member of the Mastercard or Visa network for example. From a technical point of view, payment cards must be attached to an account. The PSP, which issues the card, links these cards to technical accounts opened in its books (also known as "mirror accounts"). These accounts are opened either in the name of the partner PSP (with sub-accounts in the name of each cardholder), or in the name of each cardholder. These technical accounts are generally frontloaded either by the PSP that has a contractual relationship with the users, or by the PSP that issues the card. This is an advance payment in return for payment. Here again, according to the ACPR, the recording of funds in these accounts and the execution of the card payment transaction from these accounts mean that they qualify as payment accounts.

The stakes involved in classifying a payment account are therefore many and significant in terms of the consequences arising, in particular, from the application of PSD2 and other legislation.[298] These include, but are not limited to, the following:

(i) the requirement for authorisation (as a payment, credit or electronic money institution). Although keeping a payment account is not strictly speaking a payment service, the provision of which as a regular occupation requires authorisation,[299] keeping such an account necessarily entails the provision of certain associated payment services;[300]

(ii) the possible nullity or ineffectiveness of certain contractual clauses if they conflict with the public policy provisions of the PSD2; [301]

---

298 Such as the SEPA Regulation, for example.

299 Article 37(1) of the PSD2, transposed into Article L. 521-2 of the Financial Code.

300 G. Goffinet, *op. cit.* spec. p. 22.

301 This was precisely the subject of the substantive dispute under Austrian law which gave rise to the question referred to the CJEU for a preliminary ruling in the ING DiBa judgment cited below.

(iii) the requirement for an account servicing PSP (ASPSP) to apply strong authentication (SCA) to the account holder;[302] and

(iv) facilitating the provision of account information and payment initiation services on[303] accounts (open banking)[304] and complying with the resulting technical constraints.[305]

7.2. What is the current legal regime?

7.2.1. *In PSD2 (and other relevant European legislation)*

While the historical home of the definition of payment account is PSD1 (replaced by PSD2), this concept is also defined autonomously in other legislative texts for their own purposes.[306]

These texts have different purposes and, in some cases, different scopes of application. The PAD Directive, for example, applies only to payment accounts held by consumers and aims, in particular, to facilitate the transparency and comparability of fees relating to payment accounts, as well as the changing of accounts.[307] While, at first glance, the respective definitions of a payment account are essentially identical to those of PSD2, a closer look at the PAD is necessary. Recital 12 sets out a rule of interpretation unknown to the other texts mentioned above: "*All provisions of this Directive should concern payment accounts through which consumers are able to carry out the following transactions: place funds, withdraw cash and execute and receive payment transactions to and from third parties, including the execution of credit transfers*".[308]

---

302 Article 97(1)(a) of the PSD2.

303 Respectively, services no. 8 and 7 of Annex I of the PSD2.

304 Articles 66 and 67 of the PSD2.

305 Provided for in Delegated Regulation 2018/349.

306 See Appendix VI.

307 Article 1(1) of the PAD Directive.

308 Recital 12 of the preamble to the PAD Directive. See also, in this sense, Article 1(6) of the PAD Directive, which states: "*This Directive applies to payment accounts through which consumers are able at least to: a) place funds into a payment account; b) withdraw cash from a payment account; c) execute and receive payment transactions, including credit transfers, to and from a third party*".

7.2.2. *Case law*

In a judgment of 4 October 2018 (the "ING DiBA ruling"), referred to it for a preliminary ruling, the CJEU ruled on the definition of payment account contained in PSD1 in the light of the aforementioned PAD Directive.[309]

According to the Court, the possibility of carrying out, from an account, payment transactions in favour of a third party *or*[310] of benefiting from such transactions carried out by a third party is a constitutive element of the concept of payment account on the basis of Article 1(6) of the PAD Directive.[311] Consequently, an account from which such payment transactions cannot be carried out directly, but for which recourse to an intermediary account (for example, a deposit account) is necessary, can therefore not be considered to be a payment account within the meaning of the PAD Directive and, consequently, within the meaning of the PSD1.[312] It should be noted, however, that the concept of third party is not included in the decision itself.[313]

7.2.3. *In Member States' legislation*

A multi-jurisdictional analysis was carried out in seven countries concerning: (i) the local definition and interpretation of the notion of payment account[314] ; and (ii) any clarifications required in each jurisdiction.

---

309 CJEU, Case C-191/17, *Bundeskammer für Arbeiter und Angestellte* v ING-DiBa *Direktbank Austria Niederlassung der ING-DiBa AG*. See comment P. Storrer, "*Le rendez-vous manqué entre la CJUE et le compte de paiement*", Banque & Droit, No 182, Nov.-Dec. 2018, p. 50. See also, Bird & Bird, accessible here.

310 While the French version of the CJEU's decision uses the alternative term "ou", members of the working group point out that this is a translation problem between the French version of the decision and the original German version concerning the translation of the word "*beziehungsweise*" (respectively) in paragraph (31) of the decision. Article 1(6) of the PAD Directive, on which the CJEU relies, refers to payment accounts enabling payment transactions, including credit transfers, to be carried out in favour of a third party and being the beneficiaries of such transactions carried out by a third party. By way of example, the Italian and Spanish versions of the CJEU decision confirm this assumption in that these versions make the combination of the possibility of executing payment transactions to third parties and the possibility of receiving such transactions the criterion for characterising a payment account.

311 Recital 31.

312 Recital 32.

313 *"On those grounds, the Court (Fifth Chamber) hereby rules: Article 4(14) of [PSD1] must be interpreted as meaning that a savings account which allows for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account does not come within the concept of 'payment account'."*

314 Belgium, Germany, Italy, Luxembourg, Netherlands, Poland, Spain.

The definition of a payment account provided by PSD2 is faithfully reproduced in the seven jurisdictions surveyed. However, in four of the seven jurisdictions surveyed, the regulator or the legislator has clarified the definition of a payment account, as follows[315] :

(i) In Germany, the regulator has specified that: (x) an account qualifies as a payment account if it enables payment transactions to be carried out; (y) deposit accounts, online savings accounts and accounts held by an electronic money issuer to record the issuer's outstanding electronic money (*shadow accounts*) are not payment accounts ; and finally (z) with regard to internal and technical accounts, that they may qualify as payment accounts if they document the payment obligation between the account holder and a third party - therefore technical accounts such as credit card billing accounts or suspense accounts are not payment accounts as they are not intended for payment transactions;

(ii) In Luxembourg, the supervisor has specified that: (x) payment accounts are accounts that enable payment transactions to be carried out; and (y) electronic money accounts and wallets are payment accounts - on this point Luxembourg and Germany have a divergent position;

(iii) in the Netherlands, the regulator specified that in order to classify a savings account as a payment account, it was necessary to identify whether it was possible to carry out payment transactions via this account; and

(iv) In Poland, the legislator has specified that bank accounts and savings accounts may also be payment accounts if they are used for payment transactions.

These clarifications show that the key criterion for classifying a payment account is the possibility of carrying out payment transactions directly from the account. This position is in line with the ING DiBa ruling.

The seven jurisdictions surveyed did not identify any local case law relating to the definition of a payment account. The case law created by the ING DiBA ruling is therefore the only one applicable.[316]

The clarifications expected under PSD3 are as follows:

315 For more information, see Annex II of this report.

316 ING-DiBa ruling.

(A) for Germany and Poland[317] : no clarification is expected;

(B) for Luxembourg: the expected clarifications are those mentioned by the EBA, *e.g.*, having a more detailed definition of the payment account with criteria and/or references to specific characteristics as well as a clarification of the notion of "third party", while specifying that the new definition should ensure neutrality of the economic model and facilitate the development of different and innovative payment solutions;

(C) for the other jurisdictions, it would be appropriate to: (x) specify the technical elements of the payment account (Netherlands) and distinguish it from other types of accounts, *e.g.* current accounts (France, Italy) or savings accounts (Belgium); (y) provide a definition of mirror accounts, technical accounts or intermediation accounts (Spain, France, Italy); and (z) indicate whether certain instruments, such as prepaid cards, *wallets* and *e-wallets*, can be classified as payment accounts and therefore be subject to the payment account rules[318] (Spain).

Details of the multi-jurisdictional analysis can be found in Appendix III of this document.

7.3. HCJP recommendations

On the question of whether there should be a single definition of the payment account within the various texts that refer to it or redefine it, a consensus was reached within the working group in favour of a positive response. This definition should continue to be set out in PSD2.[319]

> **Recommendation No. 13:** The HCJP recommends retaining only one definition of payment account, which would be contained in the PSD, with the other relevant texts (in particular, the PAD Directive, the SEPA Regulation and the Interchange Regulation) having to refer to it.

Secondly, on the substance, opinions within the working group were divided.

---

317 Jurisdictions in which clarifications have been made to the definition of a payment account.

318 This would be in line with Luxembourg's current position.

319 The recommendation extends to other concepts used and sometimes redefined in these texts insofar as a single, common definition is relevant.

Some members are in favour of maintaining the *status quo*, which means that the definition of payment account contained in PSD2 should continue to be interpreted in the light of the ING DiBA ruling.

This ruling states two things: *firstly*, that an account from which payment transactions cannot be made directly, but require the use of an intermediary account, is not a payment account; and *secondly*, that the possibility of making payment transactions in favour of a third party[320] or benefiting from such transactions made by a third party is a constituent element of a payment account.

On the first point, the working group agrees that this condition is essential to the qualification of the payment account.

The second point, however, is the subject of lively debate within the group. The concept of third party is open to two different interpretations. According to one interpretation, the third party (payer or payee) would be any person who is not the holder of the account in respect of which the classification as a payment account is in question. Thus, if this account can only be funded with funds from any other account belonging to the same holder, including if the latter account is opened with another PSP, nor debited other than to the benefit of any other account belonging to that holder, then it cannot be a payment account. This interpretation should be regarded as consistent with the ING DiBA ruling, given the factual situation before the Court.[321]

According to a second interpretation, the notion of third party should be associated not only with any person other than the account holder himself, but also with the latter in respect of any account opened with a PSP other than the one holding the account in question. Thus, even in the case of payment transactions between accounts opened with separate PSPs but belonging to the same person, these accounts would all be payment accounts. This latter interpretation is favoured by the ACPR, because the first interpretation would have the effect of restricting the scope of the obligations of PSP account managers in terms of open banking.[322] The

---

320 See footnote 309.

321 See recital 12: "*ING-DiBa Direktbank Austria offers online savings accounts from which its customers can make deposits and withdrawals by means of telebanking. Those transfers must always be made via reference accounts opened in the customer's name. Those reference accounts are current accounts which the said customers may also hold with a bank other than ING-DiBa Direktbank Austria (...)*".

322 According to the ACPR, such a restriction would result in a weakening of the protection of payment service users (through massive recourse to web scrapping) as well as an additional financial risk for payment and electronic money institutions, since in the event of loss of payment service user data, these providers would be liable and would consequently have to compensate their customers. Furthermore, such a recommendation would run counter to the recommendations of the EBA as well as those of the competent European and national

FBF shares the same view, albeit with some nuances, taking the view that a payment account used to carry out payment transactions in favour of another account opened in the name of the same account holder in the same institution or in different institutions remains a payment account, provided that the regulations attached to this account do not prohibit it from carrying out payment transactions in favour of a third party or benefiting from such transactions carried out by a third party.

In conclusion, the working group's opinions remain divided on this issue. The working group therefore confines itself to recommending that the European legislator and the EBA take a closer look at the issue in order to conclude whether or not to include in the PSD a reference to the concept of third party in the definition of payment account, and to expressly take a position in the interests of legal certainty. It should be noted that, in the absence of any clarification in the text of PSD3, the concept of payment account should continue to be interpreted in the light of the ING DiBA ruling, which includes this reference to the concept of third party.

Recommendation No. 14: The HCJP recommends:

- amending PSD2 (either in the recitals or in the definition of payment account) to specify that an account from which payment transactions cannot be made directly but require the use of an intermediary account is not a payment account; and

- that the European legislator and the EBA to assess in greater depth whether the concept of third party is relevant to the definition of payment account, and to take an express stand for the purposes of legal certainty.

institutions in the area of personal data protection (the EDPB and the CNIL have recommended the introduction and use of APIs by financial players to control and secure access to financial and insurance data, even beyond data linked to payment accounts).

8. PSP LIABILITY

8.1. The one-stop shop and the division of responsibility between the ASPSP and the TPPs

8.1.1. *Issues and current legal regime*

In principle, everyone is liable for the damage they have caused by their act, negligence, or imprudence (article 1241 of the French Civil Code). By way of exception, French law provides for cases of vicarious liability (article 1242 of the French Civil Code).

These situations are justified by the desire to protect the victim. Cases of vicarious liability are precisely those in which the perpetrator of the damage is likely to be insolvent (minor child; employee; domestic servant, etc.).[323]

All cases of vicarious liability have one essential similarity: the person civilly liable exercises authority over the person who caused the damage. Liability for a third party thus appears to be a counterpart of the exercise of these powers.

These two characteristics are absent from the regime established by the PSD since, on the one side, third-party payment service providers (TPPs) do not present any particular risk of insolvency (on the contrary, the PSD has established a certain number of requirements designed to avoid this) and the Account Servicing Payment Service Provider (ASPSP) does not exercise any power or control over TPPs or over the transactions they carry out and which the ASPSP is obliged to execute.

Thus, the liability of the ASPSP cannot be based on vicarious liability or on an extensive interpretation of this principle. In its relationship with the TPPs, it is a regime that exceeds ordinary law.

When a payer denies having authorised a payment transaction initiated via a payment initiation service provider, the ASPSP is obliged to reimburse the payer immediately, and in any event no later than the end of the first working day thereafter, the amount of the unauthorised payment transaction.

While PSD2 does provide for the principle of immediate compensation of the ASPSP by the payment initiation service provider (PISP) for losses incurred or sums paid as a result of the payer's refund when the PISP is responsible for the

[323] Jérôme Julien, "*Responsabilité du fait d'autrui*", Répertoire civil Dalloz.

unauthorised payment transaction[324], the absence of a contractual relationship between them makes this principle difficult to implement.

In particular, the system should be supplemented to facilitate this compensation when an ASPSP and a PISP agree that strong authentication will be the responsibility not of the ASPSP but of the PISP.

In this situation, the working group proposes:

(i) that the PISP fully and effectively bears the consequences of the unauthorised transaction and reimburses the payer, unless the parties agree otherwise;

(ii) to provide for the contractualisation of the relationship between ASPSP and third-party PSP, by formalising in the contract the distribution of responsibility incumbent on each of the players, having first carried out a precise segmentation of the operation in question (so that *ultimately*, each protagonist may be held responsible for the part of the operation that requires his intervention, unless he provides proof of its proper execution);

(iii) that, in the event that the transaction has to be reimbursed by the ASPSP on the basis of the one-stop shop principle, the contract identifies, upstream, the responsibilities of each of the parties in a precise manner; consequently, the performance of the contract would result in the defaulting party taking responsibility for reimbursing the transaction in accordance with the obligations incumbent on it within a contractually fixed, necessarily short, period (since the ASPSP has an obligation to reimburse the unauthorised transaction on D+1). The result would be a welcome clarification of the legal obligations of the parties involved in the banking transaction.

8.1.2. HCJP recommendations

Recommendation No. 15:

- The HCJP recommends that Article 97 of PSD2 be supplemented by a sixth paragraph: (i) allowing PSPs managing accounts (ASPSP) and payment initiation service providers (PSIPs) to be able to agree that the strong authentication procedure will be the responsibility not of the ASPSP but of the PSIP; (ii) specifying that, in this context, the PSIP is liable to the user under the terms of Article 73(1) of the PSD2; and (iii) that the PSIP must inform

[324] Article 73(2), §2 of PSD2.

the user in advance in accordance with Article 52 of the PSD2. The proposed wording is as follows:

> *"6. By way of derogation from paragraph 5, payment service providers managing accounts may agree with payment initiation service providers that the latter rely on their own authentication procedures. The procedures set up by the latter must then comply with paragraphs 1, 2 and 3 respectively".*

- Consequently, Article 73(2) of the DPS2 will also have to be supplemented by a third paragraph providing in substance that it is the PSIP which bears the obligation to reimburse the payer for the amount of the unauthorised payment transaction, as follows:

> *" Where the ASPSP and the PSIP have agreed, in accordance with Article 97, that the strong authentication procedure will be the responsibility of the payment initiation service provider, it shall be the latter that reimburses to the payer, under the conditions of paragraph 1, the amount of the unauthorised payment transaction*[325] *and restores the debited payment account to the state it would have been in had the unauthorised payment transaction not taken place."*[326]

8.2. The responsibility of the ASPSP towards the customer

8.2.1. *Issues and current legal regime*

(a) An unbalanced liability regime to the detriment of PSPs

(i) The payment service user's obligations

The main provisions of the French Monetary and Financial Code which oblige the Payment Service User and which may exclude his right to reimbursement in the

[325] The revision should include an obligation for the PISP to provide users with prior information on the PISP's assumption of responsibility for the SCA and its consequences: claims for reimbursement should be directed to the PISP and not to the ASPSP.

[326] Insofar as it does not seem possible for the PISP to re-establish a payment account that it does not hold, this part of the provision should be reviewed as it does not seem consistent.

event of intentional or grossly negligent failure to comply are set out below. They are limited. The user is obliged:

(A) to take all reasonable steps to safeguard the security of its personalised security data;[327] and

(B) to immediately report the loss, theft, misappropriation or unauthorised use of their card or related data as soon as they become aware of it.[328]

(ii) PSP's obligations

For their part, and depending on the situation, PSPs are required under article 73 of the PSD2[329] to reimburse transactions reported by the payment service user as unauthorised within thirteen months of the date of debit (unless there are good reasons to suspect fraud on the part of the customer) immediately after becoming aware of them or having been informed of them, and no later than the end of the next working day.

Under article 74(2) of the PSD2[330], they must automatically reimburse unauthorised transactions in the absence of strong authentication (unless the Payment Service User has acted fraudulently).

To escape their refund obligations, they must demonstrate that the Payment Service User has committed fraud or, in the case of strong authentication, has intentionally or through gross negligence failed to fulfil his obligations (under Article 74(1) of PSD2).

Under Article 73 of PSD2, in the event of a payment transaction reported by the payment service user as unauthorised, the PSP is obliged to reimburse the payment service user by the end of the first working day thereafter at the latest, unless it has reasonable grounds for suspecting fraud on the part of the payment service user[331].

---

327 Article L. 133-16 of the Financial Code.

328 Article L. 133-17-I of the Financial Code.

329 Transposed into article L. 133-18 of the Financial Code.

330 Transposed into article L. 133-19V of the Financial Code.

331 Cf. also Recital 71 of PSD2: " *However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer*".

Under Article 72(1) of PSD2[332], where the Payment Service User denies having authorised a payment transaction or claims that the payment transaction was not executed correctly, the PSP has the burden of proving that the transaction was authenticated, properly recorded and accounted for and was not affected by a technical or other deficiency.

The PSP is therefore subject to particularly onerous constraints linked to the time allowed for reimbursing the customer (D+1) and to the burden of proof which rests on it, especially since under the terms of the second paragraph of Article 72(2) of the PSD2[333], the use of the payment instrument as recorded by the PSP is not necessarily sufficient in itself to prove that the transaction was authorised by the payer or that the payer intentionally or through gross negligence failed to fulfil his obligations in this regard. The PSP, including, where applicable, the PISP, shall provide evidence of fraud or gross negligence committed by the Payment Service User.

(b) **A "diabolical" system of proof**

(i) Under the second paragraph of Article 72(2) of PSD2, the use of the payment instrument as recorded by the PSP is not necessarily sufficient to prove that the transaction was authorised by the payer.

A payment transaction is necessarily authorised from the moment the Payment Service User has given his consent to it in the form agreed with the PSP. The context in which the Payment Service User gave his consent is irrelevant. Whether or not a transaction is authorised should only be assessed in the light of the execution of the payment transaction.

The ASPSP liability regime set out in article 73 of PSD2 applies only to unauthorised payment transactions, i.e., transactions not validated by the customer in accordance with the form or procedure set out in the contract.

Authorised payment transactions are therefore excluded from its scope.

Under Article 64(1) of PSD2, a payment transaction is authorised if the payer has given his consent to its execution. This consent is given "*in the form agreed between the payer and the payment service provider*" under Article 64(2) of the PSD2.

The form of this consent, equivalent to authorisation, cannot be unknown to the payment service user, especially as French regulations specifically require the bank, in the deposit account agreement and in the framework payment services contracts

[332] Transposed into article L. 133-23, 1° of the Financial Code.

[333] Transposed into article L. 133-23, 2° of the Financial Code.

(for example, the contract governing the use of the card or the framework agreement governing payment methods in general, including credit transfers), to communicate "*The form and procedure for giving consent to the execution of a payment transaction and for withdrawing this consent, in accordance with articles L. 133-6 and L. 133-7 of the French Monetary and Financial Code*", subject to the penalties set out in article L351-1 of the Financial Code.[334]

Furthermore, the authorised nature of a payment transaction is assessed independently of any underlying relationship. Article 4(5) of the PSD2[335] defines a payment transaction as an act, initiated by the payer or on his behalf or by the payee, of placing, transferring, or withdrawing funds, irrespective of any underlying obligation between the payer and the payee.

In practice, when a dispute arises, the courts in many cases have to determine whether the Payment Service User gave his consent to the transaction and whether, if so, the refund should therefore be disregarded. This question arises, particularly, when the Payment Service User contests the validation of an order given, in a fraudulent context or following manipulation by a fraudster.

Since the payment transaction is independent of the underlying obligation, the dispute can only relate to the consent given to the transaction, regardless of the underlying obligation. In this context, it should be considered that a payment transaction is necessarily authorised from the moment the Payment Service User has given his consent to it in the form agreed with the PSP. It does not matter in what context the Payment Service User has given his consent. Whether or not a transaction is authorised should only be assessed in the light of the execution of the payment transaction.

Finally, it should be considered that when the customer has used the methods available to him to give his consent, in particular by using one of the strong authentication devices made available to him by the ASPSP in accordance with what is agreed with the ASPSP, the transaction should be considered authorised.[336]

---

334 *Cf.* Articles L. 312-1-1-II and L. 314-12-II of the Financial Code and the amended Order of 29 July 2009 implementing these articles, relating to relations between payment service providers and their customers regarding information obligations for payment service users and specifying the main stipulations to be included in deposit account agreements and payment service framework agreements.

335 Transposed into article L.133-3-I of the Financial Code.

336 In this regard, Trib. de com. Saint Nazaire, 15 June 2022, case no. 2021001463; Trib. jud. Paris, 8 June 2022, 9th chamber 2ème section, no. RG 19/04840; 15 November 2022, no. RG 22/02540. The decisions are appended to the report (Appendix VII)

From this point of view, the recent decision handed down by the Versailles Court of Appeal is disputed by the banking industry and has not yet been finalised.[337]

(ii) Under the terms of the second paragraph of Article 72(2) of the PSD2, the use of the payment instrument as recorded by the PSP is not necessarily sufficient itself to prove that the payer intentionally or by gross negligence failed to fulfil his obligations in this regard.

The PSP, including, where applicable, the PISP, provides evidence of fraud or gross negligence committed by the payment service user.

The case law prior to PSD2 considers that the use of a secure system as required at the time of the events does not give rise to a presumption of intentional breach or gross negligence on the part of the payer.[338]

The Court of Cassation's solution[339] is particularly strict. It places the burden of proof on the bank, which is particularly difficult to prove because it depends on the information that the payer agrees to disclose, even though the PSP has computer traces reconstructing the history of the disputed payment or transaction.

Insofar as it is up to the PSP to prove fraud or gross negligence on the part of the payer, it alone cannot reconstruct the context of the fraud if the payment service user remains silent on the circumstances of the fraud, which occurred prior to the disputed transaction on media to which the PSP does not have access. The Directive does not require the payer to provide information on the context in which the fraudulent transaction was carried out,

Similarly, the negative proof of the absence of a technical deficiency required by Article 72 of the PSD2 appears particularly difficult to provide. This should be limited to proof of the absence of a technical deficiency "*detected and recorded by the bank*" that may have affected the transaction, insofar as the bank's means of action and control over the execution of the payment transaction are necessarily limited.

In the context of a payment transaction, the bank does not, for example, have control over the terminal used by the payment service user. Consequently, an obligation to prove the absence of any deficiency, even one undetectable by the bank, would be

337 CA Versailles, 28 March 2023, RG n°21/07299. The decision is appended to the report.

338 Cass. Com, 18 January 2017, no. 15-18102.

339 See also Cass. Com. 12 November 2020, no. 19-12112: the Court confirms the reasoning of the *Tribunal d'instance*, which ordered the bank to reimburse the victim of a phishing scheme, on the grounds that it had not demonstrated the absence of a technical deficiency within the meaning of article L. 133-23 of the Financial Code.

tantamount to requiring the bank to guarantee the proper functioning of elements over which it has no control.

8.2.2. *HCJP recommendations*

The issue is being discussed by the working group. According to the representatives of the banking industry, it should be expressly mentioned in the revision of PSD2 that the implementation of a strong authentication procedure enables the ASPSP to consider that the payment transaction is presumed to be authorised, since Article 73 of PSD2 is not intended to apply in this situation. However, the ACPR is opposed to the proposal to introduce a simple presumption of authorisation of a payment transaction in the event of strong authentication, considering that it would be unfavourable for the payment service user.

However, there is a consensus on the appropriateness of adjusting the D+1 refund period set out in Article 73(1) of PSD2 for transactions disputed by the payment service user. This timeframe does not allow PSPs to carry out the necessary investigations to establish suspicion of fraud or, where applicable, the user's consent to the transaction, particularly in the case of strong authentication. It could therefore be proposed to extend this period (between 5 and 15 days) so that PSPs can carry out these investigations.

Recommendation No. 16:

The HCJP recommends amending Article 73 of PSD2 to extend the period for reimbursement in the event of an unauthorised payment transaction to five (if the payment service user is a consumer) or fifteen (otherwise) working days instead of one working day as is currently the case, as follows:

> *" 1. Member States shall ensure, without prejudice to Article 71, that, in the case of an unauthorised payment transaction, the payer's payment service provider reimburses the amount of that transaction to the payer ~~immediately~~ after becoming aware of the transaction or after being informed of it, ~~and in any event no later than~~ the end of the ~~first~~ **[fifth or fifteenth**[340] **]** working day thereafter, unless the payer's payment service provider has reasonable grounds to suspect fraud and communicates those grounds in writing to the relevant national authority. Where applicable, the payer's payment service provider shall restore the*

[340] The 15-day period could be provided for when the user is not a consumer

debited payment account to the state it would have been in had the unauthorised payment transaction not taken place. This also assumes that the value date on which the payer's payment account is credited is not later than the date on which it was debited.

2. Where the payment transaction is initiated via a payment initiation service provider, the payment service provider managing the account shall refund the amount of the unauthorised payment transaction ~~immediately, and in any event no later than~~ the end of the next [fifth or fifteenth] business day, and, where appropriate, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

We also need to reposition the value of digital evidence in the legal debate.

Increased dematerialisation of the relationship between PSPs and payment service users necessarily goes hand in hand with computerised traceability of transactions carried out with the payment service user's identification and authentication details. The data and technical parameters collected by the application software used by the PSPs provide a chronological record of the transactions carried out, associated with the customer's identification details, which ensures that they can be allocated. These are the intrinsic proofs of payment transactions available to the PSP.

As the law currently stands, under Article 72(1) of the PSD2, it is up to the PSP to prove that the user, who denies having authorised a payment transaction, has acted fraudulently or failed to fulfil his obligations intentionally or through gross negligence. In this sense, the PSP must also provide extrinsic evidence.

Although proof cannot be deduced from the mere fact that the payment instrument or the personal data linked to it were used, the fact remains that the PSP's intrinsic evidence must also have its place in the demonstration of authorisation or gross negligence.

The judicial debate must make a proportionate assessment of their technical and objective existence, particularly in the absence of a declaration from the customer clarifying the precise circumstances of the fraud, or silence on the part of the customer, as the digital logs constitute proof of the transactions that took place and how they were carried out (the transaction in question was authenticated, duly recorded and accounted for and was not affected by a technical or other deficiency).

Recommendation No. 17 : The HCJP recommends amending Article 72 of PSD2 to provide that, where a payment service user denies authorising a payment transaction that has been executed or claims that the payment transaction has not been executed correctly, the PSP may provide evidence "that it did not detect a technical or other deficiency in relation to the service provided which could have affected the transaction", rather than evidence "that the transaction in question was not affected by a technical or other deficiency in the service provided by the PSP". The amendments would read as follows:

> *"1. Member States shall require that, where a payment service user denies having authorised a payment transaction which has been executed or claims that the payment transaction has not been executed correctly, the payment service provider shall bear the burden of proving that the transaction in question has been authenticated, properly recorded and accounted for* ***and ~~that it has not been affected by~~ detecting a technical or other deficiency in relation to the service provided which could have affected the transaction.***
>
> *If the payment transaction is initiated via a payment initiation service provider, the latter shall bear the burden of proving that, as far as it is concerned, the transaction in question has been authenticated and duly recorded ~~and that it has not been affected by a technical or other deficiency in the service provided by the payment service provider~~* ***and that it has not detected a technical or other deficiency in relation to the payment service it is required to provide.***

8.3. Sharing information on fraudulent IBANs

8.3.1. *Issues and current legal regime*

A key aspect of the fight against fraud to ensure the protection of our customers in the public interest is the need to consider centralising the identity of fraudsters and fraud data (IBAN of fraudsters, IP address or mobile number of fraudsters), both within the groups to which PSPs belong where applicable, or outside such groups, with other PSPs or national authorities, police where applicable. Data on a fraudster collected by a PSP should be able to be communicated to other PSPs in order to alert them.

The regulations should therefore be amended to allow PSPs to share information useful in the fight against fraud.

Combined with customer warnings and greater security for payment transactions, this ability to share information would certainly be a major step forward in the fight against fraud.

Information sharing should also provide for the PISP to be informed when a transaction cannot be carried out due to suspected fraud.

In addition to this sharing option, appropriate and proportionate rules should be laid down regarding the obligation to provide individual information to persons suspected of fraud who are the subject of personal data processing for this purpose. Informing suspected fraudsters on an individual basis poses difficulties, particularly in view of the risks of incivility and violence towards PSP employees, especially branch employees, who need to be protected. In addition, informing these people is likely to hamper the investigations carried out by the authorities (TRACFIN, judicial authorities) and ultimately run counter to the anti-fraud measures.

8.3.2. *HCJP proposals*

Recommendation No. 18: The HCJP recommends that a new paragraph (3) be added to Article 26 of the PSD2 to allow, but not require, the exchange of information between PSPs for the sole purpose of combating fraud and without professional secrecy constituting an obstacle or being enforceable, as follows:

> *"In order to ensure the security of payment transactions and the protection of users, in particular the protection of their funds against the risks of fraud, the competent authorities of the Member States shall authorise, where appropriate with the assistance of their national central bank, the exchange of information between payment service providers relating to fraud, including confidential information and personal data such as the name of the account holder and/or data enabling a payment account to be identified, and any other information likely to make it possible to detect the possible initiation and execution of fraudulent payment transactions. Payment service providers are not obliged to share this information.*

This ability to exchange confidential information between payment service providers may only be used for the sole purpose of combating fraud.

The professional secrecy to which persons working for the national central banks of the Member States or for payment service providers may be bound is not enforceable and may not prevent the sharing of confidential information.

These procedures are not subject to any obligation of result or disclosure to a third party other than a payment service provider.

The payment service provider cannot be held liable for failure to consult or share information".

9. DATA ACCESS

9.1. Access to data by TPPs and non-discrimination principle

9.1.1. *Issues and legal regime*

Under the "non-discrimination" principle in Article 36(1) of the Delegated Regulation (EU) 2018/389 (the RTS SCA)[341], the payment service user must have access to data via their account information service provider (AISP), or aggregator, as if they were going through the services made available by their ASPSP.

The working group was divided on this issue.

For the representatives of the ASPSPs, and mainly the banking industry, the scope of PSD2 and the principle of non-discrimination by PSPs need to be clarified. Indeed, the ASPSPs have noted a trend towards extending the sharing of information with PSPs to cover functions accessible via online banking services, as long as they relate to a payment account.

Thus, at the request of the banking supervisor, accounts for which the account holder has given a mandate to a third party must be included in the scope of aggregation of accounts opened in the name of this third party, even if the mandate given by the account holder to this third party does not provide for this possibility. For the ASPSPs, under PSD2, only accounts opened in the name of the same payment service user should be covered by the scope of aggregation. They consider that this extension is therefore contrary to the very definition of the account information service, which should be limited to the user's accounts.[342]

Future transactions concerning cards (including deferred debit card payments), direct debits and credit transfers also had to be made accessible to TPPs by ASPSPs, which is also contested by credit institutions regarding the definition of the account information aggregation service.

---

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

342 See the definition of the account information service in Article 4(16) of PSD2 ("*an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider ")* and Article 67(2), §d) and §f) of PSD2 *("The account information service provider shall access only the information from designated payment accounts and associated payment transactions ; not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.").*

Ultimately, for the banking industry, the information that can be shared under PSD2 must be strictly determinable. Only account balances and movements should be included in the scope of aggregation.

For the representatives of aggregators (AISP) and initiators (PISP), on the other hand, it was found that ASPSPs could use the dedicated interface (the API) to limit the data made available to TPPs. In fact, they consider that the principle of minimisation is used by the latter to hinder the quality of service of these players. For example, when several interfaces are used by the ASPSP for direct access by payment service users (a website and a mobile application), it has been observed on several occasions and for several players that the content of the API corresponded to the data of the least efficient interface. To illustrate this assertion, an example is given of a bank using 256 characters on its website and 32 on its mobile application for the message accompanying the transfer instruction. This bank considers that it is the wording of the mobile interface that should appear in the API made available to the TPP.

These factors were brought to the attention of the French competition authority, the Haute Autorité de la Concurrence, which included them in its opinion No. 21-A-05 of 29 April 2021 in the following terms: "*It is therefore clear from the above that the possession by* ASPSPs *of payment account data accessible online could give them a significant advantage over new players in the payments sector, some of whom are heavily dependent on access to such data in order to be able to operate on the market*".

With regard to data ownership, AISP representatives wished to point out that third-party services are provided to the payment service user who, as PSD2 reminds us in its definitions, is not simply the holder of a payment account, but is more broadly a payment service user, which therefore includes those to whom services are provided by PSPs in the same way as ASPSPs.[343] .

For these representatives, it is therefore necessary that the information made available to AISPs does not put them in a situation where the payment service user would criticise them for providing incorrect information compared to that provided by their ASPSP. And this is what has been observed in practice by TPPs, in specific cases where users note a difference in the information concerning the available balance and the list of transactions carried out between their ASPSP and their account aggregator.

[343] Article 4(10): "*payment service user 'means a natural or legal person making use of a payment service in the capacity of payer, payee, or both* ".

While AFEPAME understands that ASPSPs may wish to offer "value-added" information to their users, they should not be allowed to conceal from aggregators transactions or operations originated by the payment service user (whether deferred or not).

For AFEPAME, which is in favour of determining the information that can be shared in order to avoid differences of interpretation between the various banking establishments, it is essential, however, to allow the Payment Service User to consent to the sharing of his data without his ASPSP being able to stand in the way. The scope of the information that can be shared must therefore be sufficiently broad to enable any PSP (both ASPSP and AISP) to provide the various services desired by the Payment Service User.

(a) **Interpretation of the principle of "non-discrimination" and competition between service providers**

For the banking industry, the broad interpretation of the "non-discrimination" principle is detrimental to competition, freedom of trade and the investments made by ASPSPs. It considers that the principle of non-discrimination should be without prejudice to the ability of ASPSP s to maintain a certain level of innovation and to develop a competitive advantage. In its view, the principle of certain services/data being made available free of charge by ASPSPs under PSD2 should therefore be applied strictly and not extended to other services/data.

Banks' online services evolve regularly and the ASPSP does not approve of the fact that, in the name of a principle of non-discrimination that is too broadly understood, ASPSPs benefit from an unconditional, free and automatic right of access to these developments, beyond what should be strictly accessible within the framework defined by the PSD2 and its accompanying texts.[344]

---

[344] Article 36(1) of the RTS SCA: *" 1. Account servicing payment service providers shall comply with each of the following requirements:*

(a) they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data;

(b) they shall, immediately after receipt of the payment order, provide payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;

(c) they shall, upon request, immediately provide payment service providers with a confirmation in a simple 'yes' or 'no' format, whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer."

The investments made by ASPSP s to offer new functions to their users or to improve their online banks are made with the aim of satisfying their customers and in a context of competition with other service providers. The ASPSPs therefore consider that forcing them to share these services free of charge with competitors is unfair (given that access to quality data requires investment in specific infrastructures) and contrary to the principle of freedom of trade and industry and distorts competition.

For the banking industry, ASPSPs must have a guarantee that they will be able to retain the competitive advantages provided by the development of new services and innovative services. ASPSPs are therefore keen to ensure that any new service, information or data relating to the payment accounts of payment service users made available via their online banking service does not become unconditionally accessible to competitors simply because the service, information or data is accessible by the payment service user via their online banking service. They are of the opinion that the right of service providers to access certain information on payment accounts under PSD2 should not be assessed in the light of all the information available to the user on his consultation interface.

They are in favour of a mechanism to ensure that these innovative and competitive services are not included in the common core of PSD2. Failing this, the banking industry considers that this extended access will have negative effects on the ability of ASPSPs to innovate and on the development of services with added value and that, ultimately, it will lead to the costs of innovation being borne indirectly by users alone.

For the members of AFEPAME, the possibility left to the bank to choose which data is available or not in the interfaces made available to aggregators poses a major risk in terms of competition, as already indicated above.

They note that not all ASPSPs see TPPs as allies enabling them to complement the services available to the joint customers of TPPs and ASPSPs, and that some banking players are deliberately using this opportunity given to them to restrict the data available to make their services more relevant than those of aggregators. According to AFEPAME members, healthy competition between the various players should encourage them to innovate and offer more services of interest to customers rather than, on the contrary, negatively affecting the services of the other players.

AFEPAME considers that the principle of non-discrimination should be without prejudice to the ability of TPPSs to maintain a certain level of innovation and to

develop a competitive advantage. It considers that the data that should be available under PSD2 should be extended to all personal data and points out that access to data is neither automatic nor unconditional since it is based on the consent and authentication of the data owners.

For AFEPAME, TPP and ASPSP services are not competitors but complementary. In order to function, aggregation or payment initiation services need users to have accounts with ASPSPs.

For AFEPAME, it is important that any personal information, any personal data, relating to the payment accounts of the payment service user made available on his online bank becomes accessible under certain conditions. This information, this data, must be accessible by the customer on his online bank (whether through a web browser, a mobile application, or a specific ASPSP interface) and it must relate to a payment account.

This principle of "non-discrimination" will have positive effects on innovation, on the ability of ASPSPs and TPPs to innovate and on the development of services with added value. In fact, personal data is and must remain the property of users, with innovation focusing solely on the added value provided by ASPSPs and TPPs rather than simply making information available. To do otherwise would be to withhold information to the detriment of the payment service user.

AFEPAME believes that access to data should not in itself constitute an advantage. However, it agrees with the banking profession that each of the players (TPP and ASPSP) must be guaranteed to be able to retain the competitive advantages that the development of new and innovative services provides.

In conclusion, while disagreeing on the review of the principle of non-discrimination provided for in Article 36(1) of the RTS SCA, the ASPSPs and the TPPs nevertheless share the idea that a precise list of standard data, to which the TPP would have access as part of the aggregation service covered by PSD2, would be useful. The data on this list, which could be updated regularly, would be accessible to the TPPs as part of the above-mentioned service, provided that it was already available online to the payment service user and related to his payment account. However, the members of the working group do not agree on how this list should be drawn up (either by agreement or established or recognised by an official authority). The working group is therefore not in a position to propose a recommendation on this issue.

(b) Different data access rules for users depending on the status of PSP

Within the working group, the banking industry points out that although AISPs are PSPs under PSD2,[345] article 97 of PSD2,[346] does not apply to AISPs, which do not manage payment accounts on behalf of their customers. They do not offer their customers direct access (via their own API, for example) to online accounts, but to payment information that they have previously collected from one or more ASPSPs. As such, they are not subject to the USP's strong authentication requirement, which only applies to ASPSPs when customers access their online payment accounts, for example, either directly or via a AISP.

As a result, ASPSPs note that the USP benefits from access to information held by the AISP without strong authentication, whereas this strong authentication is required of the ASPSP in the case of direct access by the user to his payment account information. The customer 'journey' will therefore not be identical depending on whether the user contacts the AISP or their ASPSP. The customer journey will be smoother, as there will be no need for a strong authentication procedure if the data held by the AISP is consulted, regardless of the nature of the data, without the limitations imposed on ASPSPs.

The banking industry points out that, by contrast, the exceptions to strong authentication for access to payment account information directly from the ASPSP are strictly regulated[347] : absence of sensitive data, payment account balances, transactions carried out in the last 90 days. From the user's point of view, these differences are not consistent for ASPSPs and, among them, credit institutions, which consider that data and access to data should be secured in the same way regardless of the PSP. From the banking industry's point of view, the lack of strong authentication on the part of AISPs increases the risk of fraud and raises questions in terms of competition between these PSPs, which are subject to different rules.

For AFEPAME, it seems unreasonable to consider that the USP benefits from access to information held by the AISP without strong authentication, when on the contrary, in practice, AISP services cannot be provided if the USP does not carry out a strong authentication, at the first connection for each of his banking connections and every 90 to 180 days for each of his connections to his payment accounts. AFEPAME does not understand how banks can consider services that

345 In France, in accordance with article L. 521-1 of the Financial Code.

346 Transposed in France by article L. 133-44 of the Financial Code.

require recurring redirections to multiple strong authentications with very heterogeneous typologies and paths to be more fluid.

In any event, it considers that it is wrong to think that the services of the AISPs are not subject to the obligation of strong authentication. Even if the USP's strong authentication obligation is not binding on the AISPs, in practice their services cannot operate without a strong authentication being carried out for each of the accounts held with the ASPSP every 90 (or soon 180) days.

AFEPAME points out that AISPs would be in favour of being able to benefit from the same rules as ASPSPs, i.e., to be able to carry out strong authentication of payers and to be able to exempt them from strong authentication (in the absence of any proven risk) for 90/180 days.

9.1.2. *HCJP proposals*

The members of the sub-group disagreed on (i) the need to re-examine the principle of non-discrimination set out in Article 36(1) of the RTS SCA; (ii) the procedures for drawing up a precise list of standard data accessible to TPPs in the context of the aggregation service covered by PSD2; and (iii) the need to introduce a legal requirement for strong authentication on the part of the AISP when its USPs access the information it holds.

The members of the sub-group are therefore not in a position to propose a recommendation on these points.

9.2. Contracts would provide a framework for the delivery of services

9.2.1. *Issues and current legal regime*

(a) Services that meet the needs of the market, within the framework of PSD2 or beyond

Within the working group, the representatives of ASPSP expressed the view that they were in favour of the services, information and data accessible under PSD2 being strictly defined within the framework of a contract. This contract would clearly indicate, among the data made available by the institution on its online banking space, the list of those that specifically fall within the scope of PSD2.

Additional services, information and data that go beyond what is strictly provided for by PSD2 should be able to be offered by ASPSPs to their customers, with a view to innovation and competition between providers, and should only be accessible to other providers with the agreement of the ASPSP concerned and in accordance with

negotiated and contractually agreed terms (cf. particularly the so-called "premium" services and SEPA Payment Account Access - SPAA).[348]

The ASPSPs stress the importance of allowing each player to develop its services and new functions, notably in consideration of demand and market needs, and to contractualise them in order to make them available. In their view, it is preferable for new functions to be developed to meet market needs rather than regulatory requirements. The service provided for in Article 65 of PSD2, consisting of requiring ASPSPs to confirm to payers' PSPs the availability of funds in the event of card payments, is an example of a service developed to meet a regulatory requirement and which was not ultimately used. The ASPSPs point out that this service represents lost investment and revenue. They therefore consider that this pitfall could have been avoided if the PSPs themselves, by contract, had chosen to develop and offer services that precisely met expectations. For ASPSP, the fact that the service is free of charge and that it is impossible to enter into contracts with TPPs has meant that it has not been possible to broaden the exchange of information with TPPs, or to establish a *business model*, even though the implementation costs have been significant.

In this respect, the ASPSP consider that the principles set out in Articles 8 and 9 of the proposed regulation on data[349] should be supported.

Article 8 states firstly that the provision of data by a "data holder" to a "data recipient" must be carried out under fair, reasonable and non-discriminatory conditions, in a transparent manner and on terms agreed between the parties. A binding contractual clause may govern access to and use of the data, liability and remedies.

In addition, the ASPSPs raise the issue of compensation for the provision of data by ASPSPs to TPPs. From this point of view, they note that Article 9 of the above-mentioned draft regulation lays down a principle of reasonable compensation for the provision of data between data holders and a data recipient. The ASPSP support a compensation principle applicable regardless of the size of the recipient company (small, medium or large). However, for them, a simple compensation approach is not sufficient. Compensation, which should be contractually agreed and freely

---

348 See European Payments Council (EPC), SEPA Payment Account Access : "*The SEPA Payment Account Access (SPAA) scheme covers the set of rules, practices and standards that will allow the exchange of payment accounts related data and facilitates the initiation of payment transactions in the context of 'value-added' ('premium') services provided by asset holders (i.e. Account-Servicing Payment Service Providers (ASPSPs)) to asset brokers (e.g. Third Party Providers (TPPs)).*"

349 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final.

negotiated by the parties (without reference to guidelines or recommendations from the authorities), should be based on the cost of making the data available, but also on the actual value of the data communicated. The ASPSP point out that the databases and the communication channel that enable data to be transmitted to a third party mobilise substantial financial resources. It does not seem fair that the corresponding cost should be borne exclusively by the ASPSP when the AISPs are using this data as part of a commercial activity.

For its part, AFEPAME is opposed to PSD2 data being subject to the need for a contract, as this proposal by the banking profession would contravene the principle that everyone is free to dispose of their data under the conditions they wish. This principle is also enshrined in Article 20(2) of the GDPR.[350]

AFEPAME also fears that some account-keeping institutions will not sign up to such a contract, just as some have chosen not to use an API as the dedicated access interface for TPPs.

For AFEPAME, it is not simply the agreement of the ASPSP that should legitimise such access, but the consent of the payment service user.

On the other hand, AFEPAME is not opposed to the possibility of contracting for additional services, information and data, which would go beyond what is strictly provided for by the PSD2, even if this is less obvious as far as "data" is concerned. Indeed, even if the data outside the scope of PSD2 seems to meet the principle of portability set out above and should not be subject to the need for a contract, it is rather the API format of provision for which third parties are prepared to contract.

AFEPAME does not understand why the banking profession considers that contractualisation is impossible today. It also points out that it has always been in favour of remuneration for additional services, and that having failed to reach agreement on this issue, it doubts the assumption that free services would be the real stumbling block.

For AFEPAME, the obligation of contractualisation give an advantage to the institution holding the data when negotiating the terms of such a contract and contravene the principles of fairness and non-discrimination set out above. Furthermore, if this seems applicable to data other than personal data, it contravenes the GDPR as far as personal data is concerned.

---

350 "*In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.*"

AFEPAME wishes to point out that personal data is the property of USPs and not of banks or even aggregators. Considering the value of personal data and charging for simple access to this data would contravene the principle of the GDPR, which is the "free circulation of personal data".

(b) **Contractualisation via standards in the form of schemes?**

For ASPSPs, setting up the equivalent of a scheme at European level would certainly enable the regulatory authorities to reach a consensus on the interpretation of the provisions of PSD2.

They consider that establishing a regulatory framework and legitimising contractualisation between PSPs would strengthen security aspects and make it possible to hold each player accountable, in a market that serves customers. For these service providers, this would make it possible to govern certain services by contract, or in consideration of market demand by a kind of adhesion contract, in the form, for example, of a European payment scheme for what is already regulated by the PSD2 (proposal to refer to the SEPA schemes with a view to transposing certain elements).

In addition, by allowing contractualisation, ASPSPs consider that they could open up functionalities requiring specific developments and new information for TPPs (e.g. information concerning the deferred nature of card transactions, savings accounts).

From their point of view, an *ad hoc* contractual agreement would also provide an appropriate framework for the services offered: security measures, exclusivity, intellectual/industrial property on Premium Services.

Given these observations, the ASPSP representatives emphasise that the initiative supported by the EPC, work on which is currently underway, aimed at launching a new payment system (SEPA Payment Account Access - SPAA) with the objective of offering new value-added services (premium services), meeting real customer needs and distributed within a business model that is fair between participants,[351] could meet these objectives.

Ultimately, the ASPSPs consider that these contractual standards could organise: (i) access to information and exchanges between PSPs, including reasonable compensation for the costs of making data available and maintaining infrastructures; (ii) security measures; (iii) intellectual/industrial property rules; (iv)

[351] The SPAA scheme provides for invoicing for access to data shared by ASPSPs (see SEPA Payment Account Access (SPAA) Scheme Rulebook EPC012-22 / Version 1.1, available here).

the procedures for obtaining customer consent, which must be clear to all three parties (the ASPSP, the TPP and the account-holding customer who is a payment service user); (v) where applicable, the responsibilities of the PSP in charge of the SCA and the division of responsibilities between service providers; (vi) the principles for remunerating additional services; and (vii) the procedures for resolving disputes.

For the members of AFEPAME, contractualisation is already legitimate and despite all the energy already put into defining such contracts or schemes, the banking profession has always been dissatisfied with the results of the work undertaken and reluctant to finalise them.

AFEPAME points out that deferred card payment transactions are information within the scope of PSD2. Despite tripartite discussions and the opinion of the Banque de France on the subject, only a small number of players in the banking industry consider that this information is not part of PSD2 data (in practice, all other account-holding institutions include this data in their PSD2 APIs). Even though their customers are dissatisfied and explicitly wish to be able to consent to the sharing of this information, these players are maintaining their positions and taking advantage of the introduction of APIs to lock in the services of aggregators. AFEPAME wishes to point out that while each ASPSP has had to incur costs and development work to implement the APIs, for payment aggregators and initiators, as many costs and developments as ASPSPs have been imposed on them.

AFEPAME would be in favour of a change to the directive that would allow ASPSPs and AISPs to agree by contract that the strong authentication procedure is the responsibility not of the ASPSP but of the AISP. The contract would consequently reorganise the rules and responsibilities defined by PSD2.

9.2.2. *HCJP proposals*

As the members of the sub-group disagreed on the contractual framework for the provision of services, the working group was unable to make a recommendation on the subject.

9.3. **Access to data by CTs: the need to develop the use of APIs?**

9.3.1. *Issues and current legal regime*

The legal framework for payment aggregation and initiation activities and the requirement for a secure method of communication between players are a major contribution of PSD2.

To meet this last requirement, the French banks point out that, in November 2015, they initiated an interbank initiative to meet a dual objective: to secure access to data and to provide a simple, innovative solution - in other words, to offer a common API to prevent security measures from being circumvented, in particular by sharing the user's password, which should only be known by the person generating it and the person using it.

The French banks maintain that they have worked on the definition, development and production of an API standard that fully complies with the requirements of the Framework Directive and the RTS (security standards, based on a standardised and secure access method open to all players), both in terms of equal access for all players and security for customer data. As a result, by proposing a common standard, the French banks consider that they have greatly facilitated the work of the TPPs in connecting to banking information systems (a single standard provides access to all the French banks' APIs).

(i) The French banking community points out that it was the first in Europe to publish the technical specifications for its API back in July 2017.

(ii) With this API-based approach, PSD2 has laid the foundations for the technical exchange of data within a secure framework.

When implementing APIs, a great deal of work was carried out to comply with the requirements imposed by the directive (level 1 text) and the RTS (security standards, based on a standardised and secure access mode open to all players), both in terms of equal access for all players and security for customer data (level 2 texts).

The representatives of the French banks taking part in the working group consider that the interbank approach has enabled all the TPPs to connect to all the French banks using a single standard. However, they regret the following aspects of these developments and the work carried out with the TPPs and the national supervisory authority:

(A) a lack of clarity between the RTS, the guidelines and the details of the requirements, which have been added over time, have made the texts very difficult to implement and, on many subjects, have been subject to multiple interpretations. AFEPAME shares this point of view;

(B) passive connections that generate costs, with several banks continuing to observe TPPs connecting to their APIs without generating any activity whatsoever (the sole purpose of the API calls being to check its availability, without generating any activity); and

(C) a disappointing rate of use of APIs, albeit on the increase, and the continued practice of web scrapping.

The banking industry therefore proposes that the HCJP recommend the development of APIs, on the *one hand*, by making their use compulsory, at least as soon as an API is offered by the ASPSP, on the *other hand*, by prohibiting access to a user's data when the access methods circumvent security measures and rely in particular on the sharing of the USP password made available and communicated by the ASPSP and, *finally*, by making API certification levels more flexible (objective criteria set by the directive): a de facto solidarity has been established between the three APIs resulting from PSD2 as prescribed by the regulations. Thus, an exemption is only authorised if the three APIs (i.e. payment account information; payment initiation; and CBPII[352]) comply with the EBA's guidelines.[353] According to representatives of the banking industry, these guidelines lack proportionality and do not differentiate between, on the one hand, a consumer or non-professional user and, on the other hand, a professional customer or a legal entity, for which the security requirements and operating methods are different, which creates a *de facto* obstacle to the compliance of certain APIs dedicated to the payment initiation service. It is on this point that API certification levels should be made more flexible.

For its part, AFEPAME would like to point out that web scrapping and API are two technologies that enable payment aggregation and initiation services, but that sharing the user's password is not specific to web scrapping, and that some European banks have chosen to implement APIs based on this same authentication method. And the reverse is also true, as web scrapping is perfectly possible without password sharing.

Thus the authentication phase and the interface use phase are two separate things and, consequently, the following four methods are possible:

(1) web scrapping using user identifiers ;

(2) API by using a redirection to the ASPSP so that the latter can issue an API access token;

(3) API via the use of user identifiers; and

---

352 Service for confirming the availability of funds provided for in Article 65 of the PSD2.

353 EBA, "*Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)*", EBA/GL/2018/07 4, December 2018.

(4) Web scrapping by using a redirection to the ASPSP so that the latter can issue an access token to the user interface.

Furthermore, considering that the API is more secure than web scrapping means considering that the interfaces delivered by banks to their users are not sufficiently secure (screen scrapping is by design subject to exactly the same security measures as users when they use the interfaces directly).

Since the effective implementation of DPS2 with regard to data access, and the fact that the TPPs provide their APIs, the TPPs can only observe the heterogeneity of the APIs made available by the ASPSPs. In practice, the APIs of two ASPSP s are much more different than their direct interfaces (websites available to customers). The STET standard is very open and free, allowing each bank to implement it according to its own rules.

As already indicated by AFEPAME on a recurring basis for several years, the choice made by ASPSP to limit the data accessible via the API requires TPPs to maintain access to the back-up mechanism for access to other data consented to by customers.

If a ASPSP no longer wishes to use web scrapping, it can do so - it's simply a question of will.

AFEPAME is not in line with the three recommendations of the banking profession:

(A) the first point is already relevant, since it is the ASPSP that chooses the interface that must be used by the TPPs (cf. article 31 of the RTS SCA);

(B) the second point is merely the reciprocal of the first and is therefore of no interest as such in terms of the banking industry's choices. On the other hand, some ASPSPs (French and European) have chosen the "authenticated" web scrapping or API "with Embedded Authentication" method as a response to article 31 of the RTS SCA, and this recommendation would put them in difficulty.

(C) Finally, AFEPAME can only note the real difference in quality between "certified" IPAs (exempt from the back-up mechanism) and recommends that the current level be maintained. All the more, French banks have mostly reached this target.

AFEPAME recommends that all USP personal data be made available in order to better differentiate between direct user access and TPP access.

9.4. **HCJP recommendations**

In the absence of consensus at this stage, the working group is not in a position to propose recommendations, and further work is required.

10. ACCESS TO DATA BY PSPS AND PROTECTION OF PERSONAL DATA

10.1. An approach that complies with the principles set out in GDPR

10.1.1. *Issues and current legal regime*

It is essential to focus on the purposes of the operation and to share data solely for these purposes.

Thus, on the question of access to payment account data held by a user specifically, in accordance with the GDPR, the personal data processed relating to the user's accounts must be adequate, relevant, and limited to what is necessary with regard to the purposes for which they are processed (data minimisation).

Consequently, a clear delimitation of the types of data concerned in the context of TPP access and the resulting limitation of the unnecessary circulation of data would ultimately fall within the scope of compliance with the principle of minimisation and would be in the interests of data protection.

AFEPAME is perfectly in line with the FBF on this point and points out that it is the responsibility of the payment service user to delimit the data concerned relating to their payment accounts and not the ASPSP. Under no circumstances should this principle of minimisation be used to hinder the services of ASPSPs.

On this approach of compliance with the principles laid down by the European Data Protection Regulation, the banks stress the importance of the consent of the user of an account information service. In the interests of sound management of their rights and effective protection of their personal data, they propose that Article 67 of PSD2 be supplemented to allow users of an account information service to revoke their consent to a SIPP ("right of revocation"). They support the introduction of a dashboard in banks' online interfaces, so that USPs can have a centralised channel for identifying at source the TPPs with whom they share their data and easily revoke consents that are no longer current.

AFEPAME considers that such a possibility would presuppose that the ASPSP and the AISP could agree by contract that the strong authentication procedure is the responsibility not of the ASPSP but of the AISP, the contract reorganising accordingly the rules and responsibilities defined by the PSD2. In the absence of an agreement on this point between the PSPs[354] , the AFEPAME cannot support the approach proposed by the banks, considering that the interest for the USP to be able

[354] See above.

to revoke the consent given to the ASPSP only makes sense if the accesses are maintained over time without the intervention of the ASPSP in its renewal.

10.1.2. *HCJP recommendations*

In the absence of a consensus, the working group is therefore not in a position to propose a recommendation on this point.

10.2. **Revision of Article 94 of the PSD2 Directive**

10.2.1. *Linking the provisions of Articles 94.2 of the PSD2 and 6.1 of the GDPR*

(a) **Issues and legal regime**

As concerns the articulation with the GDPR, Article 94.2 should be deleted.

The processing of personal data by PSPs is not based solely on the user's consent, but more often on other grounds such as performance of the contract, compliance with a legal obligation or legitimate interest.

On the other hand, consent must remain a possible legal basis.

Chapter 4 of Title IV of PSD2 (Article 94) deals with (personal) data protection. The objectives of this article are: (i) to emphasise the importance of a proper framework for the processing of personal data by PSPs; and (ii) to ensure a proper link between the PSD2 and specific regulations relating to the processing of personal data (in particular the GDPR).

This desire on the part of the European legislator is also reflected in the recitals of thePSD2:

(A) Recital 89: Where personal data is processed for the purposes of this Directive, the precise purpose should be specified, the relevant legal basis referred to, the relevant security requirements laid down in Directive 95/46/EC complied with, and the principles of necessity, proportionality, purpose limitation and proportionate data retention period respected. Also, data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of this Directive.

(B) Recital 93: payment initiation service providers and the account information service providers on the one hand and the account servicing payment service provider on the other, should observe the necessary data protection and security requirements established by, or referred to in, this Directive or included in the regulatory technical standards.

In principle, the inclusion in the texts of a link between PSD2 and the GDPR is to be welcomed. However, the current wording of Article 94 raises several problems of interpretation and application (i) the term "personal data" is not defined in Article 4 of PSD2. However, in order to avoid any confusion with other terms with a similar resonance (e.g. sensitive payment data, personalised security data), a reference to the definition in the GDPR would be useful; and (ii) Article 94(2) is unclear and appears to be redundant in relation to other provisions of PSD2 and the GDPR.

The EDPB clarifies that consent given under Article 94(2) should not be confused with consent under Article 6(1)(a) of the GDPR:

> *"Explicit consent under Article 94(2) PSD2 should therefore be regarded as an additional requirement of a contractual nature in relation to the access to and subsequently processing and storage of personal data for the purpose of providing payment services and is therefore not the same as (explicit) consent under the GDPR " (point 36 EDPB opinion). In particular, consent under Article 94 § 2 does not constitute a legitimate basis for processing personal data within the meaning of the GDPR and is additional to the consent potentially required under the GDPR.[**Commentaire à Laura** : Je ne trouve pas le paragraphe surligné dans l'opinion citée de l'EDPB]"*

While it is easy to understand that consent under Article 94(2) is distinct from consent under the GDPR, it is hard to see what the function/use of this paragraph is:

(1) if the function of this paragraph is to ensure the protection of the user's personal data, this objective is already fully ensured by the reference to the specific texts/the GDPR in Article 94(1). What is more, paragraph 2 is confusing because it could be thought (wrongly and contrary to what is stated in the GDPR) that the legitimate basis for processing personal data under the PSD2 is in all circumstances the user's consent;

(2) if the function of this paragraph is to ensure that the user gives his contractual consent to the provision of payment services (in the sense of common civil law), the article is badly drafted and redundant. If this is its true function, the article should not refer to the processing and storage of personal data, but to "general" contractual consent, and should not be included in a chapter entitled "Data Protection". Moreover, Articles 64, 66 and 67 already address the issue of consent in the sense of civil law.

For all these reasons, the working group recommends deleting Article 94 (2) of the PSD2.

(b) **HCJP Recommendation 1**

> **Recommendation No. 19:** The HCJP recommends the deletion of Article 94(2) of PSD2 (which provides that PSPs shall only have access to personal data necessary for the performance of their payment services with the explicit consent of the payment service user), as it is not justified in the light of the provisions of the GDPR.

10.2.2. *The delimitation of data protection responsibilities between PSPs*

Article 94 of PSD2, which makes the processing of personal data for the purposes of the Directive subject to compliance with Directive 95/46/EC and the national rules transposing that Directive, applies to all PSPs, including PSPs.

However, in the context of data access, the division of responsibilities regarding data processing, minimisation of processing, etc., is not always clear.

If the PSP managing the account is usually a controller within the meaning of the GDPR, the TPP is also required to comply with the rules of the GDPR.

Certain obligations are also specified by the PSD2 in this respect (see for example Articles 66 and 67: obligation to access only the data necessary for the provision of the service). However, in the event of a data leak or other case of non-compliance with the GDPR - how is the issue of liability resolved?

This point could be dealt with as part of the contract between the TPP and the PSP holding the account.

For AFEPAME, each of the players is responsible for the data processing they carry out. The TPP is not the subcontractor of the ASPSP. The concept of data controller should not be dealt with in PSD2 and should remain within the remit of the GDPR. Moreover, the GDPR does not provide for the need for a contract to govern the responsibility of each party (this is only one of the possible legal bases). For AFEPAME, it is not necessary to put in place a contract for an aggregator to be liable for a data leak of which it is at the origin, or for its failure to comply with the GDPR.

(a) **Payment data and sensitive data within the meaning of the GDPR**

(i) Issues and legal regime

The working group disagrees with the European Data Protection Committee's (EDPS) almost automatic assimilation of payment data to sensitive data within the meaning of the GDPR[355] .

Indeed, data relating to financial transactions are not mentioned in Article 9(1) of the GDPR as a special category of personal data. Nevertheless, the EDPS Guidelines[356] seem to presume that data relating to financial transactions could be special categories of personal data within the meaning of the GDPR, on the grounds that financial transactions may reveal sensitive information about a data subject and that the chances that a service provider processing information about a data subject's financial transactions also processes special categories of personal data are considerable. Consequently, the EDPS recommends at least identifying and categorising precisely the type of personal data that will be processed and carrying out an impact assessment, which is normally only required under the GDPR when a type of processing, taking into account its nature, scope, context and purposes, is likely to result in a high risk to the rights and freedoms of natural persons. These recommendations do not seem to us to be justified in the case of processing in connection with the provision of payment services t and financial services in general, and go beyond what is provided for in the GDPR and the PSD2. The inference of sensitive data within the meaning of Article 9(1) of the GDPR from a USP's financial transaction data would require the data controller to intentionally and specifically carry out data processing for the purpose of inferring sensitive data within the meaning of the GDPR. In such a situation, data controllers would in fact apply the conditions required by Article 9 of the GDPR (obtaining the explicit consent of the data subject unless an exemption applies). However, where data relating to financial transactions is not processed to derive sensitive data within the meaning of the GDPR, then Article 9(1) of the GDPR should not apply, as such data does not by its very nature constitute sensitive data within the meaning of the GDPR. A principle of this type is retained in Recital 51 of the GDPR with regard to photographs, thus ruling out the systematic assimilation of processing including a photograph to processing of sensitive data within the meaning of the GDPR[357] , a principle which should also apply to processing in connection with the provision of

355 Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person , data concerning health or data concerning a natural person's sex life or sexual orientation, constitutes processing of sensitive data within the meaning of the GDPR.

356 Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 2.0, adopted on 15 December 2020.

357 The processing of photographs should not systematically be considered as constituting the processing of special categories of personal data, given that these only fall under the definition of biometric data when they are processed using a specific technical method enabling the unique identification or authentication of a natural person.

payment services. The Working Party also notes that the technical measures recommended by the EDPS, which are particularly difficult to implement in practice, would be likely to have a negative effect on the protection of the USP's personal data, in that their implementation would necessarily involve the processing of sensitive data.

Consequently, to avoid any confusion, as PSD2 includes a definition of "sensitive payment data"[358] , the working group recommends a new formulation and definition (where appropriate) of this concept, to distinguish it from that of "sensitive data" within the meaning of the GDPR.

(ii) HCJP recommendation

> **HCJP Recommendation No. 20:** The HCJP recommends replacing the concept of "sensitive payment data" defined in Article 4(32) of PSD2 with that of "protected payment data" and having the following definition: "*data, including personalised security data, which are likely to be used to commit fraud and which require an appropriate level of protection*".

10.3. Access to data and links with eIDAS

10.3.1. *Issues and legal regime*

(a) **In its proposal for a regulation,[359] the European Commission envisages the possibility, through the use cases currently being studied, of a payment function in the DIW, in addition to the identification function. This revision of the eIDAS Regulation[360] could therefore make it compulsory for PSPs to accept the DIW as a third-party authentication**

[358] Article 4(32): "'*sensitive payment data' means data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data*;".

[359] Proposal for a Regulation of 3 June 2021 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

[360] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

solution that must be offered (in competition with the other authentication methods offered by the PSP)The problem of liability

Now, under PSD2, when a payment is initiated, the ASPSP checks the SCA solution used.

In the future, with identification carried out via the DIW (and therefore in the hands of the Member States), the ASPSP will no longer be in control of the SCA solution when the USP chooses to use the DIW as a strong authentication solution. Liability issues will therefore arise in the event of identity theft and fraudulent transactions.

(b) **The problem of traceability**

Another problem is that, as the draft text for the revision of eIDAS currently stands, Member States do not have the option of tracing the use of DIWs. In the case of payment initiation, PSD2 requires dynamic authentication ("*dynamic linking*", or dynamic link between the given transaction, amount and beneficiary)[361]. This will no longer be possible.

(c) **The operational consequences of introducing a payment function in the DIW in addition to its identification function.**

As indicated by the three European banking associations in their public statement of 11 April 2023[362], the use of the DIW as a payment authentication solution would require considerable investment not only in the financial sector, but also for the payment acceptance network as a whole. This could result in disproportionate costs for merchants and service industries that accept card payments. The banks consider that it would be preferable to capitalise on the existing authentication solutions put in place following PSD2, which must remain legible and interactive with customers in the digital space.

In view of the above, the members of the banking industry participating in the working group are in favour of excluding DIW as a payment authentication solution from the scope of the revised eIDAS, which would avoid the difficulties, liability and traceability problems mentioned above. As AFEPAME does not agree on this last point, the sub-group cannot propose this recommendation.

---

361 See article 97(2) of the PSD2: "With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which **dynamically link the transaction to a specific amount and a specific payee**."

362 See "European Credit Sector Associations call for removing payments from the scope of the Digital Identity Regulation".

10.3.2. *HCJP recommendation*

Recommendation No. 21: The HCJP recommends :

- concerning strong user authentication (SCA) and digital identity wallets (DIW): considering that the ASPSP cannot be responsible for a technical identification and SCA solution over which it has no control and which is imposed on it by the regulations, the revision of PSD2 could provide that in the event of the use of a third-party solution such as the DIW, the user's consent to the execution of payment transactions cannot be contested by the latter with the ASPSP. At best, in the event of a dispute, the ASPSD may only be required to provide assistance in recovering the funds from the beneficiary's PSP;

- the requirement for dynamic strong authentication required by PSD2 at the initiation of the payment transaction will have to be compatible with the authentication solution proposed by DIW and imposed on ASPSP; and

- with regard to the relationship between the respective revisions of PSD2 and the eIDAS Regulation, given the impact of the draft revision of the eIDAS Regulation on payments, it seems essential to ensure consistency between the revision of this text and that of PSD2. Consequently, it should be recommended that the revision of PSD2, which will have to take account of the revision of the eIDAS Regulation, should only take place once the revision of the eIDAS Regulation has been fully stabilised.

APPENDIX I – GLOSSARY

ACPR	French Prudential Supervision and Resolution Authority (*Autorité de contrôle prudentiel et de résolution*).
AISP	Account information service provider.
AML/FT	Anti-Money Laundering and Countering the Financing of Terrorism.
API	Application programming interface.
ASPSP	Account servicing payment service provider.
CJEU	Court of Justice of the European Union.
COBO	Collection on behalf of.
CPCE	French Code of civil enforcement procedures (*Code des procédures civiles d'exécution*).
CRD	Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.
CRR	Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.
Digital Euro Proposal	Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro.
DIW	Digital identity wallet.
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area.
eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
EMD1	Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions.
EMD2	Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.
EMI	Electronic money institution.
ESMA	European Securities and Markets Authority.
EU	European Union.
Financial Code	French Monetary and Financial Code (*Code monétaire et financier*).
GDPR	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.
HCJP	Legal High Committee for Financial Markets of Paris (*Haut Comité Juridique de la Place Financière de Paris*).
ING DiBa Ruling	CJUE, C-191/17, *Bundeskammer für Arbeiter und Angestellte* v ING-DiBa Direktbank Austria *Niederlassung der* ING-DiBa AG.

Interchange Regulation	Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.
MAR Regulation	Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.
MiCA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
PI	Payment institution.
PISA	Eurosystem oversight framework for electronic payment instruments, schemes and arrangements.
POBO	Payment in behalf of.
PSD3 Proposal	Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC.
PSIP	Payment initiation service provider.
PSR Proposal	Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010.
PSP	Payment service provider.
PSU	Payment service user.
ROBO	Reception on behalf of.
SCA	Strong customer authentification.
SEPA Regulation	Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business

	requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009.
TSP	Technical service provider.
TPP	*Third party provider*.

APPENDIX II – COMPOSITION OF THE WORKING GROUP

PRESIDENT:

- **Frédérick Lacroix**, Partner, Clifford Chance, member of the HCJP

REPORTERS:

- **Hélène Kouyaté**, Counsel, Clifford Chance
- **Laura Chambeaud**, Lawyer, Clifford Chance

MEMBERS:

- **Charlotte Ast**, Deputy Head of the Sustainable Finance, Company Law, Accounting and Corporate Governance Office, Treasury Directorate General
- **Louise Baroin**, Lawyer, Kramer Levin Naftalis & Frankel
- **Mathilde Bonneau**, Senior manager, Government relations EMEA, PayPal
- **Sylvie Bertin-Lê**, Legal counsel, BNP Paribas
- **Nathalie Campagne**, Litigation counsel, BNP Paribas
- **Caroline Cartereau-Lima**, Legal counsel, Payments, Crédit Agricole Payment Services
- **Aurore Chevron**, Legal counsel, Payment services, Crédit Mutuel
- **Sophie Clément**, Legal counsel, La Banque Postale
- **Mia Dassas**, Partner, Allen & Overy
- **Marie Daulny**, Litigation counsel, Fortuneo
- **Maxence Delorme**, Director of Legal Affairs, AMF
- **Pierre Françon**, General Delegate, Association of Payment and Electronic Money Institutions (AFEPAME)
- **Gérard Gardella**, General Secretary, HCJP
- **Thomas Gousseau**, Linxo

HCJP - 9 rue de Valois 75001 Paris - Tel: 33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

- **Evelina Gratianu**, ACPR
- **Anne-Victoire d'Herbecourt**, Fintecture
- **Catherine L'Hostis**, Legal counsel, Group Legal Department, BPCE
- **Muriel Kah**, Crédit Mutuel
- **Hélène Lair**, Société Générale
- **Daniel Laiter**, Regulatory counsel, BNP Paribas
- **Severine Loretti**, Legal counsel, BNP Paribas
- **Alexandre Loyer**, Mangopay
- **Alexandra Marais**, ACPR
- **Delphine Marchand**, PSL Counsel, Allen & Overy
- **Francesco Martucci**, Associate Professor, Université Paris Panthéon-Assas
- **Paulo Mendes**, Head of Product Legal & Regulatory Affairs, Swile
- **Jérôme Raguenes**, Director of Digital, Payments and Operational Resilience, French Banking Federation
- **Pauline Robin**, Lawyer, Allen & Overy
- **Myriam Roussille**, Associate Professor, University of Le Mans and Director of the Le Mans Institute of Judicial Studies
- **David Sabban**, Directeur général du Trésor, adjoint à l acheffe du bureau Banfin4
- **Pierre Storrer**, Partner, Storrer & Associés
- **Jerome Traisnel**, CEO, Slimpay
- **Hubert de Vauplane**, Partner, Kramer Levin Naftalis & Frankel
- **Jonathan Vincent-Lafont**, BNP Paribas
- **Stéphane Yvon**, Legal Affairs and Compliance, French Banking Federation

APPENDIX III – MULTI-JURISDICTIONAL ANALYSES

1. MULTI-JURISDICTIONAL ANALYSIS OF THE CRITERION OF TERRITORIAL SCOPE ADOPTED IN VARIOUS MEMBER STATES

Member state	Normative text	Official doctrine or case law	Comments
Germany	None	None	BaFin takes into account the physical location of service provider in Germany (licence are triggered even if the licensable activity is conducted in parts on German territory) and/or domicile or residence of client (*i.e.*, ultimate recipient of the licensable services) in Germany and/or location of accounts used for settling the payments in Germany [363] .
Poland	None	None	No official doctrine from the Polish regulator. The KNF maintains a public warning list where it lists entities which in the KNF's view carry out activity in breach of the licensing requirements (typically the licensing requirement applies if a licensable activity is carried out "in the territory of Poland") and there are offshore entities on that list. This means that the KNF concluded that a given entity carries out activity in the territory of Poland. Unfortunately, the KNF does not provide explanation what were the basis for reaching

[363] Ref. BaFin cross-border note available here, which is accepted by the courts; the cross-border note is also applied to payment services; see also legislative reasoning BR-Drs. 827/08, p. 77 et seq.

			that conclusion. It is therefore difficult to say when, according to the KNF, the activity subject to authorisation is carried out on the territory of Poland.
Spain	None	None	The Bank of Spain has not officially taken any position on this matter. In certain cases, they have followed the "characteristic performance" approach[364] when determining the place of provision of banking services (thus including payment services), but its stance has been rather opportunistic based on the specific circumstances and the Bank of Spain's officers in charge of the case. However, considering: 1. the increasing number of market players (mainly PIs and EMIs) providing payment / e-money services based on purely digital solutions (both locally and on a freedom to provide basis); 2. that, pursuant to the Spanish implementation of the E-Commerce Directive (Directive 2000/31/CE[365]) and the Distance Marketing of Consumer Financial Services Directive (Directive 2002/65/EC[366]), "information society services" (including those which qualify as "financial services") provided by EU-based service providers are deemed provided in Spain (on a freedom to provide basis) when targeted to Spain-based consumers;

364 Commission interpretative Communication, Freedom to provide services and the interest of the general good in the Second Banking Directive, 10 July 1997.

365 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), available here.

366 Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, available here.

			3. EBA's Opinion on the nature of passport notifications regarding agents and distributors under PSD2, EMD2 and AMLD5[367]; 4. EBA's Report on potential impediments to the cross-border provision of banking and payment services[368]; 5. the convenience of applying consistent criteria to entities supervised by the Bank of Spain providing banking services (including payment services) and investment services for which the solicitation test is legally imposed; and 6. that the CRD6 Proposal now contemplates the "solicitation test" (in line with MIFID2), We have detected a certain tendency of the Bank of Spain to take into account the fact that Spanish residents are the target addressees of the services provided by the foreign payment services provider. Nonetheless, until a change in banking and/or payment services regulations takes place, it seems to us that the Bank of Spain will continue not to take a formal view on this.

[367] Opinion of the European Banking Authority on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD), 24 April 2019, available here.

[368] EBA Report on potential impediments to the cross-border provision of banking and payment services, 29 October 2019, available here.

France	None	None	The ACPR considers that payment services are provided in France when a payment service provider addresses French residents in order to offer them its services, in particular by reference to the EBA's doctrine.[369]
Italy	None	Bank of Italy Supervisory Instructions for Banks dated 17 December 2013, No. 285 and Bank of Italy Regulation on transparency dated 22 June 2012.	The Bank of Italy considers that payment services are provided in Italy when a payment service provider addresses Italy based clients in order to offer them its services.
Luxembourg	The law of 5 April 1993 on the financial sector, as	None	In Luxembourg payment services are mainly covered by two laws: the FSL (which essentially transposes the CRD and MiFID in Luxembourg) and the PSL (which transposes the current PSD). The FSL covers payment services as they are part of the general banking services (cf. point 4 of Annex I to the CRD). The PSL is the main law covering payment services in Luxembourg.

369 EBA calls on financial institutions to finalise preparations for the end of transitional arrangements between the EU and the UK, 29 July 2020; and CJEU, 10 May 1995, Alpine Investments, C-384/93, §21 and §22, ; CJEU, 6 November 2003, Gambelli *and others*, C-243/01, §53.

	amended (FSL) Law of 10 November 2009 on payment services, as amended (PSL) CSSF Circular 11/515 (Circular)		<u>Cross-border approach to EEA institutions:</u> The Luxembourg financial sector regulator CSSF traditionally applies in practice a characteristic performance approach in relation to the provision of banking, including payment services, when it comes to the determination whether services are provided in Luxembourg by a foreign EEA institution not established in Luxembourg or whether a Luxembourg institution provides service in another Member States on a freedom of services basis. The CSSF would in principle apply EU law positions (Commission interpretative Communication — Freedom to provide services and the interest of the general good in the Second Banking Directive (97/C 209/04) (the "Communication"), relevant CJEU case law, EBA GLs). Customer location may also be a criterion the CSSF may take into account, especially with regards to consumers (as it has recently done in relation to the provision of MiFID investment services under the Luxembourg MiFID third country firm regime). There are no official positions published by the CSSF on the topic. The position in relation to EEA institutions is in particular relevant for assessing the need for a freedom of services passport (in relation to payment services either under the FSL (for credit institutions) or the PSL (for payment institutions). <u>Cross-border approach to non-EEA institutions:</u> In accordance with Art. 32 (5) of the FSL, a third country firm not having an establishment in Luxembourg which provides banking (other than MiFID investment services) is required to obtain a license where one or more of their agents come to

			Luxembourg occasionally and temporarily, notably to collect deposits or other repayable funds from the public or to provide any other banking services. The Circular (currently marked on the CSSF website as subject to review) provides further guidance on the interpretation of Art. 32 (5) of the FSL, including among others, that: - 'coming to Luxembourg' requires that one or more agents, employees or other representatives of the non- EEA entity move in person (i.e. physically) to Luxembourg; and - non- EEA professionals who have clients in Luxembourg do not ipso facto carry out their activities on the territory of Luxembourg, but that the characteristic performance of the banking service or part of such performance has to take place in Luxembourg. In respect of this 'characteristic performance' approach, the Circular refers to the principles set out in the Communication. Accordingly, no licensing requirement will be triggered for these services if they are provided on a cross-border basis without a physical presence (this includes also employees or agents travelling from time to time to Luxembourg) of the relevant service provider entity in Luxembourg and/or without characteristic performance of the service (or part thereof) taking place in Luxembourg. These elements (or the absence thereof) should be assessed on a case by case basis. The PSL does not expressly provide for a licensing requirement for institutions based in a third country wishing to provide payment services to clients in Luxembourg on a cross-border basis i.e. where they have no permanent and stable commercial set up or place of operation in Luxembourg (even where such services are provided through the engagement of agents). Under the PSL, only third-country payment institutions or

			electronic money institutions wishing to establish a branch in Luxembourg are subject to licensing requirements (see Art. 22 and 24-16 of the PSL). The CSSF has, by means of press releases raised the attention of the market to the communications on Brexit of EU authorities, including with relevance for payment services EBA's communication "EBA calls on financial institutions to finalise preparations for the end of the transitional arrangements between the EU and the UK"[370].
Netherlands	None	None	(c) The Dutch Financial Supervision Act (Wet op het financieel toezicht ("**Wft**")) (which implements the European Payment Services Directive (EU/2015/2366 ("PSD2")) imposes an authorisation requirement on the provision of payment services in the Netherlands on a commercial basis, as follows. - Entities which have their registered seat in the Netherlands should apply for a license in the Netherlands; - Entities which have their registered seat in a Member State of the European Economic Area should apply for a license in such Member State (and which will then come with passporting rights for the entire European Economic Area, including the Netherlands). (d) The Dutch Central Bank (DNB) has provided the following guidance[371] on when it considers payment services being provided

[370] The EBA calls on financial institutions to finalise preparations for the end of the transitional arrangements between the EU and UK, 29 July 2020.

[371] DNB, "provision of payment services", 29 mai 2020.

			in the Netherlands: "The following aspects, whether or not combined, serve as indications suggesting the provision of payment services are aimed at the Netherlands: 1. the actual establishment of agreements for the provision of payment services with Dutch residents; 2. the use of the Dutch language by the payment service provider; 3. the payment service provider makes clear that its services are aimed at Dutch residents; 4. the payment service provider refers to Dutch legislation and regulations or to the Dutch tax system; 5. the payment service provider refers to contacts in the Netherlands; 6. the payment service provider directly addresses Dutch residents." It will depend on the actual fact pattern (taking into account the above considerations) whether the payment services will be considered to be provided in the Netherlands.

2. MULTI-JURISDICTIONAL ANALYSIS OF TECHNICAL SERVICE PROVIDERS

(a) Germany

Are payment systems (VISA, Mastercard, etc.) exempt from the application of PSD2 (exemption for payment systems (art. 3(h) of PSD2, technical service provider (art. 3(j)), other exemption)? If so, how?
We are not aware of any such guidance and card systems are not established in Germany.

(b) Spain

Are payment systems (VISA, Mastercard, etc.) exempt from the application of PSD2 (exemption for payment systems (art. 3(h) of PSD2, technical service provider (art. 3(j)), other exemption)? If so, how?
Although the Bank of Spain has not, to our knowledge, issued any guidance on this matter, it seems to assume that card schemes would be covered by the "technical provider" exclusion provided under Art. 3(j) of PSD2. However, based on our most recent experience, card schemes have been expanding their suit of products and depending on the specific arrangements with PSP, they may be entering into possession of funds.

(c) Italy

Are payment systems (VISA, Mastercard, etc.) exempt from the application of PSD2 (exemption for payment systems (art. 3(h) of PSD2, technical service provider (art. 3(j)), other exemption)? If so, how?

These exemptions have been implemented into Italian law and they are a mere copy-paste of the relevant PSD2 provisions (Art. 2(2)(h) and (l) of Legislative Decree no. 11/2010).

(d) **Luxembourg**

Are payment systems (VISA, Mastercard, etc.) exempt from the application of PSD2 (exemption for payment systems (art. 3(h) of PSD2, technical service provider (art. 3(j)), other exemption)? If so, how?
The Luxembourg legislator has not "*gold-plated*", but copied the text of the exemptions in art. 3 of the PSD2. Therefore, it would depend on the actual business set-up whether a payment scheme activity qualifying as payment service can benefit from an exemption under the technical service provider, payments systems (requiring meeting the PSD2 definition thereof) and/or other exemptions or not.

(e) **Poland**

Are payment systems (VISA, Mastercard, etc.) exempt from the application of PSD2 (exemption for payment systems (art. 3(h) of PSD2, technical service provider (art. 3(j)), other exemption)? If so, how?
defining the rules for the functioning of payment schemes and responsible for making decisions related to the functioning of such schemes require a licence from the National Bank of Poland (subject to exemptions); based on the definition, a payment organisation “defines the rules” and “makes decisions”, I do not see anything that would exempt it from payment services regulations if it actually provides payment services (and not only “defines the rules” and “makes decisions”) but this would require detailed.

3. MULTI-JURISDICTIONAL ANALYSIS OF INTRA-GROUP EXCLUSION

(a) Germany

Do payments/receipts of funds made by a group entity on behalf of other entities in the same group ("payment-on-behalf"/"POBO", and "collections-on-behalf"/"COBO") to third parties outside the group fall within the scope of the exclusion of intra-group transactions provided for in Article 3(n) of PSD2?	**Source**
Yes, it's complicated. The intra group exemption does not apply where one group entities make or receives payments to persons outside the group. However, there is a counter exemption agreed between BaFin and the Association of German Treasurers pursuant to which you may still fall under the intra group exemption if this only relates to treasury functions (such as pooling structures) and all entities involved are subject to the same risk management	Link to the BaFin website available here.

(b) **Spain**

Do payments/receipts of funds made by a group entity on behalf of other entities in the same group ("*payment-on-behalf*"/"POBO", and "*collections-on-behalf*"/"COBO") to third parties outside the group fall within the scope of the exclusion of intra-group transactions provided for in Article 3(n) of PSD2?	**Source**
Yes, Spanish law made a verbatim implementation of the intra-group exclusion set out in Art. 3(n) PSD2 in relation to which the Bank of Spain has not, to date, issued specific guidance. As a consequence, the scope seems to be circumscribed to payment transactions carried out "between" companies of the same corporate group. In relation thereto, it is worth noting that the use of the expression "collection of payment orders" in the last sentence of Recital 17 of PSD2, instead of the expression "collection of funds" or "collection of proceeds of payment transactions", could lead the Bank of Spain to consider that one the "remittance" of payment orders (not funds) would be excluded. However, a number of Spanish companies are centralising COBO/POBO payments based on a different interpretation of the intra-group exemption and we are not aware of sanctions being imposed by the Bank of Spain.	Article 4 (n) of Law 19/2018, of 23 November 2018.

(c) **Italy**

Do payments/receipts of funds made by a group entity on behalf of other entities in the same group ("payment-on-behalf"/"POBO", and "collections-on-behalf"/"COBO") to third parties outside the group fall within the scope of the exclusion of intra-group transactions provided for in Article 3(n) of PSD2?	**Source**
Yes, the intra-group exemption set out in art. 3(n) PSD2 has been implemented into Italian law and it is a mere copy-paste of the relevant PSD2 provision.	Art. 2(2)(p) of Legislative Decree no. 11/2010.

(d) **Luxembourg**

Do payments/receipts of funds made by a group entity on behalf of other entities in the same group ("payment-on-behalf"/"POBO", and "collections-on-behalf"/"COBO") to third parties outside the group fall within the scope of the exclusion of intra-group transactions provided for in Article 3(n) of PSD2?	**Source**
Uncertain. The Luxembourg legislator has not gold-plated, but copied the text of the exemption in art. 3(n) PSD2. There is to the best of our knowledge no explicit official guidance on this exemption from the CSSF.	Art. 3 (1)(n) of the Law of 10 November 2009 on Payment Services, as amended.

(e) **Poland**

Do payments/receipts of funds made by a group entity on behalf of other entities in the same group ("payment-on-behalf"/"POBO", and "collections-on-behalf"/"COBO") to third parties outside the group fall within the scope of the exclusion of intra-group transactions provided for in Article 3(n) of PSD2?	**Source**
The exemption in Article 3(n) PSD2 has been transposed into Polish law as follows (machine translation): "*The provisions of the Act [on payment services] do not apply to (…) payment transactions and ancillary services referred to in Art. 74 sec. 1 point 1, closely related to the provision of payment services, carried out between a parent company and a subsidiary or between subsidiaries of the same parent company, with the participation of a provider belonging to the same group*".	N/A

4. MULTI-JURISDICTIONAL ANALYSIS OF COLLECTION ON BEHALF OF THIRD PARTIES IN DIFFERENT MEMBER STATES

(a) Germany

Does the activity of collecting funds on behalf of third parties fall within the scope of PSD2?	**Source**
Yes, potentially. Depending on the type of activity, the activity of collecting deposits on behalf of third parties could be classified as the collection of deposits, the transfer of funds, etc.	KAGB, KWG, ZAG

(b) Spain

Does the activity of collecting funds on behalf of third parties fall within the scope of PSD2?	**Source**
Yes, the Bank of Spain has not, to date, issued specific guidance regarding this topic. However, this activity would typically fall within the scope of payment services #6 of PSD2 (i.e., money remittance). However, depending on how it is technically implemented, it may also be considered to fall under payment service #5 of PSD2 (i.e., acquiring). This	Article 1.2 (e) and (f) and Article 4 (b) of Act 19/2018, of 23 November 2018. EBA Q&A.

Does the activity of collecting funds on behalf of third parties fall within the scope of PSD2?	Source
understanding is in line with the answer provided by EBA to Question 2020_5216 and Question 2020_5099. The "commercial agent" exclusion (Art. 3 (b) of PSD2) would only be available if and only if the party acting as fund-collector was effectively authorised to "negotiate or conclude the sale or purchase of goods or services on behalf of" the payee; i.e., acting within the scope a broader mandate granting it a certain degree of discretion over the "sale or purchase of goods or services" (see answer provided by EBA to Question 2020_5355) The general Spanish market is not fully aware of this interpretation and, therefore, many companies still provide "collection services" without being duly authorised.	

(c) **Italy**

Does the activity of collecting funds on behalf of third parties fall within the scope of PSD2?	Source
Uncertain, but probably yes. There is no useful explicit guidance under the existing Italian regulatory framework governing the provisions of	N/A

payment services. That said, given the features of this service, it is likely to be treated as one or more payment services as defined under PSD2.	

(d) **Luxembourg**

Does the activity of collecting funds on behalf of third parties fall within the scope of PSD2?	**Source**
Yes, unless exempted by law. The EBA has clarified on two different occasions that "The receipt and forwarding of funds qualifies as a payment service according to Article 4(3) of Directive (EU) 2015/2366 (PSD2) in conjunction with Annex I PSD2, unless an exclusion according to Article 3 PSD2 is applicable." It can be expected that the CSSF, which has not published explicit administrative practice on the question, will align its practice with the EBA and consider the activity, if carried out as a service to a third party, as a payment service, which falls under the PSD2 implementing law's regime, unless a statutory exemption is available. The qualification of the activity will depend on the specific circumstances (e.g. money remittance without payment account involvement?, cash collected placed on a client's payment account?, service to payor and/or payee?, acquisition of payment transactions?).	EBA Q&A - Question 2020_5216 ; Question 2020_5099.

(e) **Poland**

Does the activity of collecting funds on behalf of third parties fall within the scope of PSD2?	**Source**
No KNF position on the collection of funds on behalf of third parties. There has been no discussion of this issue among market players or in the literature. Polish law is not particularly specific in this respect.	N/A

5. MULTI-JURISDICTIONAL ANALYSIS OF THE CONCEPT OF PAYMENT ACCOUNT IN DIFFERENT MEMBER STATES

(a) Germany

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
German law did not make any goldplating to the definition of "payment account" set out under Article 4 §12 of the PSD2. Under German law, a "payment account" is defined as "*an account held in the name of one or more payment service users which is used for the execution of payment transactions*".[372]	**Yes**. The German financial supervisory authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* ("**BaFin**")) has published a circular pertaining to ZAG (the "**Circular**").[373] In section 2, paragraph 2 (a) (aa) of the Circular, BaFin describes	**No.** To the best of our knowledge, there is no German case law relating to the definition of "payment account". We are only aware of the judgment of the Court of Justice of the European Union..	**No**.

[372] Sec. 1 para. 17 of the German Payment Services Supervisory Act (*Zahlungsdiensteaufsichtsgesetz* ("**ZAG**")).

[373] Link here (in German language only).

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
	the following characteristics of a payment account: • not just an internal, technical account; rather, it also documents an obligation (of the payment service provider) to owe money to another (account holder) in order to pay it to the account holder or to a third party; • represents the claims and liabilities between the payment services user and the payment service provider (bookkeeping and invoices) and determines the payment service user's claim against the payment service provider;		

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
	• (online) savings accounts that can be used with a corresponding reference account are not payment accounts; • the mere provision of money for safekeeping does not establish a payment account; • the current account (*laufende Rechnung*) only becomes a payment account if it is also intended for the execution of payment transactions[374] ;		

[374] Note on 'payment transactions': this term is defined as (i) the deposit of cash against the creation of book money, (ii) the payment of cash against the release of book money, and (iii) the transfer of book money.

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
	• other pure deposit accounts as well as pure credit and credit card billing accounts, mere deposits and purely internal, technical clearing, interim and profit accounts are also not payment accounts because they are not intended for payment transactions; • the shadow accounts kept with an e-money issuer, which reflect the circulating e-money of this issuer, do not meet the requirements of the payment account either.		

(b) **Belgium**

What is the definition of "payment account" in local legislation?	**Has the local supervisory authority issued guidance on the legal definition of a "payment account"?**	**Has case law provided any guidance on the definition of a "payment account"?**	**Have you identified a clarification of this definition that could be useful in the context of PSD3?**
Belgian law did not make any goldplating to the definition of a "payment account" set out under Article 4 §12 of the PSD2. Under Belgian law, a "payment account" is defined as: "an account held in the name of one or more payment service users which is used for the execution of payment transactions". [375]	**No.**	**No.** To the best of our knowledge, there is no local case law relating to the definition of a payment account.	The Belgian Financial Sector Federation ("***Febelfin***"), representing the Belgian banking industry, has not issued any statements on the interpretation of the concept "payment account". It should however be noted that the applicability of the PSD2 with regards to "savings accounts" often remains a topic of discussion in Belgian doctrine. These discussions particularly relate to the question of whether a "savings

[375] Article 2, 18° of the Law of 11 March 2018 on the legal status and the supervision of payment institutions and electronic money institutions, access to the activity of payment service provider, access to the activity of issuing electronic money, and access to payment systems.

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
			account" might qualify as a "payment account". In order to assess whether a savings account qualifies as a "payment account", Belgian doctrine generally refers to the following criteria as defined in the Belgian preparatory works implementing the PSD1: **Purpose of the account** - An account should, a priori, not be considered as a payment account in the case where making a few payments is only an accessory function of an account that is used mainly for other purposes, such as saving. **Limitations** - In case legislative or contractual limitations are of

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
			such a nature that it would de facto be impossible to use the account for the execution of payment transactions on a regular basis, the accounts should not be considered as payment accounts. In addition, Belgian doctrine refers to EU guidance (former Q&A of the European Commission on the PSD1) stating that a savings account in which the account holder can place funds whenever he/she wants, and from which he/she is also able to withdraw funds whenever he/she likes without any restrictions (e.g. penalties), characterises as a payment account.

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
			More recent Belgian doctrine refers to the judgment of the Court of Justice of the European Union dated 4 October 2018. Based on these criteria, some Belgian doctrine note that the interpretation of the Belgian legislator is not identical to the EU guidance. Whereas the Belgian legislator focuses on the main purpose of the account, the European legislator seems to focus on the possibility to use the account to execute and receive payment transactions to and from a third party. In the light of the above, a more specific definition of “payment account” could be useful.

(c) **Spain**

What is the definition of "payment account" in local legislation?	**Has the local supervisory authority issued guidance on the legal definition of a "payment account"?**	**Has case law provided any guidance on the definition of a "payment account"?**	**Have you identified a clarification of this definition that could be useful in the context of PSD3?**
Spanish law did not make any goldplating to the definition of a "payment account" set out under Article 4 §12 of the PSD2. Under Spanish law, a payment account is defined as *"an account held in the name of one or more payment service users which is used for the execution of payment transactions*."[376]	**No.** There are no specific guidelines from the Bank of Spain ("**BoS**") on this matter. However, when the BoS refers to payment accounts, it mentions them as equivalent to bank deposits or current accounts in which various debits and credits are made[377], which does not grant much certainty to the definition itself. Additionally, the BoS has published a list of the most	**No.** the best of our knowledge, there is no local relevant case law providing insight into the definition of payment account.	With the aim of providing certainty to the definition, some local market operators are of the opinion that a future definition of payment account under the PSD3 framework should clarify whether mirror accounts, as well as intermediate operational payment accounts such as omnibus accounts, can be considered as payment accounts in some cases. Likewise, the definition should take into account whether certain

376 Article 3.11 of Royal Decree-Law 19/2018, of 23 November, on payment services.

377 "*La cuenta de pago es el equivalente al depósito o cuenta a la vista bancaria en la que se practican diversos adeudos y abonos*"), as per Section "2. Criteria of the Department of Conduct of Entities" of the BoS annual Complaints Report, link here, in Spanish language only.

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
	representative services linked to a payment account, that may be useful where evaluating whether an specific product can be considered as a payment account or not[378]: • maintaining the account; • provision of payment instruments linked to customer's account; • arranged and unarranged overdraft; • standing order; • cash withdrawal; • text alert services;		payment instruments such as prepaid cards working as wallets, as well as e-wallets should have the treatment and the consideration of payment accounts in some cases.

[378] Link here, in English language.

What is the definition of "payment account" in local legislation?	Has the local supervisory authority issued guidance on the legal definition of a "payment account"?	Has case law provided any guidance on the definition of a "payment account"?	Have you identified a clarification of this definition that could be useful in the context of PSD3?
	• cheque negotiation and clearing; and • return of cheques.		

(d) **Italy**

What is the definition of "payment account" in local legislation?	**Has the local supervisory authority issued guidance on the legal definition of a "payment account"?**	**Has case law provided any guidance on the definition of a "payment account"?**	**Have you identified a clarification of this definition that could be useful in the context of PSD3?**
Italian law did not make any goldplating to the definition of "payment account" set out under Article 4 §12 of the PSD2. Under Italian law, a payment account is currently defined as "*an account held with a payment service provider by one or more payment services users to execute payment transactions*"[379] .	**No.**	**No.** We are not aware of consolidated case law providing for clarifications and/or further elaborating on the definition of payment account as defined under Italian law.	In Italy, the need to properly identify and clarify the specific characteristics and features characterising the bank account, on one hand, and the payment account, on the other hand, both in terms of applicable regulatory regime and intermediaries providing the accounts, is a quite hotly debated issue among the legal scholars. We are of the view that in the context of the PSD3, the criteria distinguishing payment account from bank account should be clearly identified.

[379] According to Article 1(l) of Legislative Decree no. 11 of 27 January 2010 (*i.e.*, the decree that implemented PSD2 in Italy).

(e) **Luxembourg**

What is the definition of "payment account" in local legislation?	**Has the local supervisory authority issued guidance on the legal definition of a "payment account"?**	**Has case law provided any guidance on the definition of a "payment account"?**	**Have you identified a clarification of this definition that could be useful in the context of PSD3?**
Luxembourg law did not make any goldplating to the definition of payment account set out under Article 4 §12 of the PSD2. Under Luxembourg law, a payment account" is defined as a "*an account held in the name of one or more payment service users which is used for the execution of payment transactions*"[380] .	**Yes.** The *Commission de Surveillance du Secteur Financier* (the "**CSSF**") has published on 3 June 2020 a Q&A in relation to the definition of payment account.[381]	**No.** To the best of our knowledge, there is no local case law on the definition of a payment account.	No other considerations except as those flagged in Section 1.4 of the EBA Opinion dated 23 June 2022[382] .

380 Article 1(5) of the Luxembourg act dated 10 November 2009 on payment services (the PS Act 2009).

381 Link available here.

382 Link available here.

(f) **Netherlands**

What is the definition of "payment account" in local legislation?	**Has the local supervisory authority issued guidance on the legal definition of a "payment account"?**	**Has case law provided any guidance on the definition of a "payment account"?**	**Have you identified a clarification of this definition that could be useful in the context of PSD3?**
Dutch law did not make any goldplating to the definition of a "payment account" set out under article 4 §12 of the PSD2. Dutch law defines the payment account as "*an account held in the name of one or more payment service users which is used for the execution of payment transactions*"[383] .	**Yes,** the Dutch Central Bank (*De Nederlandsche Bank, "***DNB***"*) and the Authority for Financial Markets (*Autoriteit Financiële Markten, "***AFM***")* have published a Q&A on the question if savings accounts characterise as payment accounts. **"Question:** *Do savings accounts qualify as payment accounts, in the sense that account information or payment initiation service*	**No.** To our knowledge, there is no local case law in the Netherlands concerning the definition of a payment account.	It would be useful to have technical specifications for determining when an account should be considered a payment account.

[383] Article 1:1 of the Dutch Financial Supervision Act (**DFSA**). In Dutch: "betaalrekening: op naam van een of meer betaaldienstgebruikers aangehouden rekening die voor de uitvoering van betalingstransacties wordt gebruikt, als bedoeld in artikel 4 van de richtlijn betaaldiensten;".

	providers must be allowed access to these accounts if they have the account holder's explicit consent, as stipulated in Articles 66 and 67 of the PSD2? **Response:** *It depends on the restrictions on depositing, transferring and withdrawing funds in and from the accounts whether the savings accounts qualify as payment accounts – to which account information or payment initiation service providers (third parties) must be allowed access in accordance with Articles 66 and 67 of the PSD2. Savings accounts that allow unrestricted funds transfers to other accounts qualify as payment accounts (see Notes).* *In the Netherlands, most savings accounts have one or more fixed contra accounts. On 4 October*		

	2018, the Court of Justice of the European Union (CJEU) ruled that savings accounts with a fixed contra account were not to be regarded as payment accounts. This ruling was made on the basis of the PSD1. In the meantime, the European Commission has made it clear to the Dutch Ministry of Finance that this Court ruling – with the caveat that ultimately only the European Court can give a definitive interpretation – also applies under the PSD2, as the definition of "payment account" in Article 4(12) of the PSD2 remains the same as in Article 4(14) of the PSD 1. Savings accounts with one or more fixed contra accounts are therefore not covered by the PSD2, according to the European Commission. DNB and the AFM will follow this position.		

	Providers of savings accounts with a fixed contra account can allow account information service providers, subject to the consent of the individual account holders, to access savings accounts outside the PSD2. Savings accounts providers may do so on the basis of agreements with the third parties in question – provided they are clear about this towards their account holders. *We wish to point out, however, that competition rules may apply to the question whether access must be provided to third parties. Restricting such access may be in violation of competition rules. This could also apply to savings accounts with a fixed contra account. In the Netherlands, the Authority for Consumers & Markets*		

	(ACM) oversees compliance with these rules. *Finally, we remind market parties that the General Data Protection Regulation (GDPR) must be complied with when processing personal data including personal data related to savings accounts. In the Netherlands, the Dutch Data Protection Authority (AP) supervises compliance with these rules.* ***Notes**:* *Section 1:1 of the Financial Supervision Act (Wet op het financieel toezicht – Wft) defines a payment account as an account in the name of one or more payment service users that is used to effect payment transactions. Section 1:1 of the Wft subsequently defines the*		

	term payment transaction as the depositing, transferring or withdrawing of funds, irrespective of whether there are any underlying obligations between the payer and the payee. *In 2008, the European Commission stated in a Q&A document that savings accounts qualify as payment accounts if the holder can deposit, transfer and withdraw funds without any additional intervention or consent from his payment service provider.* *Possible restrictions that prevent the holder from freely depositing and withdrawing funds are:* *- The payment service provider applies administrative charges or contractually defined*		

	penalties for depositing, transferring or withdrawing funds. *- Depositing funds requires administrative action (e.g. concluding a new agreement)* *- Depositing, transferring or withdrawing of funds is limited to e.g. a specific number of times or to specific periods.* *Fixed-term deposits for instance do not qualify as payment accounts, according to the Commission, since it is not possible to withdraw funds from such accounts instantly and without restrictions".*		

(g) **Poland**

What is the definition of "payment account" in local legislation?	**Has the local supervisory authority issued guidance on the legal definition of a "payment account"?**	**Has case law provided any guidance on the definition of a "payment account"?**	**Have you identified a clarification of this definition that could be useful in the context of PSD3?**
Polish law did not make any goldplating to the definition of a "payment account" set out under Article 4 §12 of the PSD2, there are only minor linguistic discrepancies. Under Polish law, a payment account is defined as "*an account held for one or more users used to perform payment transactions, whereby a payment account is also understood as a bank account and an account of a member of a cooperative savings and credit union, if these accounts are used*	**Yes.** Under the Polish definition, the following clarification was added: "*a payment account is also understood as a bank account and an account of a member of a cooperative savings and credit union, if these accounts are used to perform payment transactions.*" This wording is not included in the PSD2 definition but it should be assumed that it is logically true also on the basis of the PSD2.	**No.** To the best of our knowledge, there is no local case law relating to the definition of the payment account.	**No.** To the best of our knowledge, there is no clarification required by the actors in the payment area.

to perform payment transactions"[384]			

[384] Article 2 (25) of the Polish Payment Services Act.

APPENDIX IV – PROVISIONS OF PSD2 FOR WHICH THE LEGISLATOR DECIDED NOT TO OPT FOR FULL HARMONISATION

Provision	Content	Details
Art. 2	Scope	
Art. 8 § 3	Own funds Member States or their competent authorities may choose not to apply Article 9 of the directive to payment institutions which are included in the consolidated supervision of the parent credit institution pursuant to the CRD (if the conditions laid down in Article 7 of the CRR are met).	Article 9 deals with the calculation of own funds
Art. 32	Exemptions / Payment services providers Member States may exempt or allow their competent authorities to exempt payment services providers (referred to in points (1) to (6) of Annex I) from the procedure and conditions of Chapter I, Title II of the directive (except registration, EBA register, designation of competent authorities, professional	Article 5 Applications for authorisation Article 6 Control of the shareholding Article 7 Initial capital Article 8 Own funds Article 9 Calculation of own funds Article 10 Safeguarding requirements

	secrecy, right to apply to the courts, exchange of information). Annex I 1. services for placing cash on a payment account and operating a payment account 2. cash withdrawal services from a payment account and operations for the operation of a payment account 3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: a) direct debits, including one-off direct debits; b) payment transactions through a payment card or a similar device; c) execution of credit transfers, including standing orders. 4. Execution of payment transactions where the funds are covered by a credit line for a payment service user: a) execution of direct debits, including one-off direct debits; b) execution of payment transactions through a payment card or a	Article 11 Granting of authorisation Article 12 Commmunication of the decision Article 13 Withdrawal of authorisation

	similar device; c) execution of credit transfers, including standing orders. 5. issuing payment instruments and/or acquiring of payment transactions 6. money remittance	
Art. 38 § 2	Transparency of conditions and information requirements for payment services 2. Member States may apply the provisions of this title to microenterprises in the same way as to consumers.	
Art. 42 § 2	Derogation from information requirements for low-value payment instruments and electronic money For national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in Article 42(1) and may increase them up to EUR 500 for prepaid payment instruments.	Art. 42 § 2: Payment transactions that do not exceed EUR 30 or that either have a spending limit of 150 euros, store funds of less than EUR 150

Art. 55 § 6	Termination of framework contracts Member States may lay down more favourable provisions for payment service users.	
Art. 57 § 3	Information for the payer on individual payment transactions Member States may require payment service providers to provide information on paper or on another durable medium at least once a month free of charge.	
Art. 58 § 3	Information for the payee on individual payment transactions Member States may require payment service providers to provide information on paper or on another durable medium at least once a month free of charge.	
Art. 61 §§ 2 and 3	Scope of Title IV Rights and obligations in relation to the provision and use of payment services	Article 102: ADR procedures for the settlement of disputes between payment service users and payment service providers concerning the rights and obligations

	Member States may provide that Article 102 shall not apply where the payment service user is not a consumer. 3. Member States may provide that the provisions in this title are applied to microenterprises in the same way as to consumers.	
Art. 74 § 1 al. 2	Payer's liability for unauthorised payment transactions By way of derogation from Article 73, the payer may be obliged to bear losses up to EUR 50 in respect of any unauthorised payment transaction resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.	Subparagraph 2: The first subparagraph shall not apply if : a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, excepted where the payer has acted fraudulently; or (b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.
Art. 86	National payment transactions For national payment transactions, Member States may provide for shorter	

	maximum execution times than those provided for in this section.	

APPENDIX V – Overview of solutions adopted in European texts

Text	Provisions concerned	Comments
AIFMD[385]	Chap. VII, spec. art. 37	Authorisation of non-EU AIFMs intending to manage EU AIFs and/or market AIFs managed by them in the Union.
CRD /CRR[386][387]	None	Doctrine of the European Commission (characteristic performance).[388]
CRD6	Art. 21c(2)	Reverse solicitation criterion (see MiFID/MiFIR).
CSDR[389]	Article 25.	A third-country central securities depository (CSD) may not provide certain core services relating to financial instruments constituted under the law of a

385 Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, available here.

386 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 relating to the taking up and pursuit of the business of credit institutions and the prudential supervision of credit institutions and investment firms, available here.

387 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, available here.

388 European Commission, "Interpretative Communication of the Commission, Freedom to provide services and the interest of the general good in the Second Banking Directive ", SEC(97) 1193 final, spec. p. 6 and 7, available here

389 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories, and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, available here.

		Member State or set up a branch if it does not have a recognition decision from ESMA.
EMIR[390]	Art. 25(1)	A CCP (*central counterparty*) may not provide clearing services to clearing members established in the EU if it has not been granted recognition by ESMA. See also the European Commission's doctrine on the provision of clearing services by a third-country CCP (central counterparty) to branches established in third countries of clearing members established in the European Union.[391]

[390] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, available here.

[391] European Commission, DG Internal Market and Services, "*Practical implementation of the EMIR framework to non-EU central counterparties (CCPs)*", Brussels, 13 May 2013, p. 1: "*EU clearing members accessing non-EU CCPs through local branches will only be able to continue to do so if those non-EU CCPs are recognised under EMIR. As EMIR only applies to entities established in the EU, this does not apply when EU banking groups access non-EU CCPs through local subsidiaries. In contrast to local branches, these local subsidiaries are not considered as EU clearing members.*"

MiFID /MiFIR[392][393]	MiFID, Chap. IV, Art. 42; MiFIR, Title VIII, Art. 46	Reverse solicitation criterion. In other words, the third-country service provider must demonstrate that it has been solicited by the customer and that no steps have been taken by the service provider to solicit the customer or induce the customer to solicit the service provider.
MiCA	Recital (51)	Reverse solicitation criterion (see MiFID/MiFIR).

[392] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, available here.

[393] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012, available here.

APPENDIX VI – DEFINITIONS OF PAYMENT ACCOUNT

Text	Definition of a payment account
SEPA Regulation	Article 2(5): "*an account held in the name of one or more payment service users which is used for the execution of payment transactions* ".
PAD Directive	Article 2(3): "*an account held in the name of one or more consumers which is used for the execution of payment transactions ".*
Interchange Regulation	Article2(22): "*an account held in the name of one or more payment service users which is used for the execution of payment transactions, including through a specific account for electronic money as defined in point 2 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council*".

APPENDIX VII – LIST OF LEVEL 1 AND 2 EUROPEAN TEXTS REFERRING TO THE CONCEPT OF PAYMENT ACCOUNT

Reference	Object	Relationship with the "payment account" concept
Regulation (EU) 2022/2065	Regulation on a single market for digital services.	Online platforms facilitating contracts between consumers and professionals must obtain payment account details.
Directive 2014/17/EU	Directive on mortgage loans	Home loan lenders may require borrowers to open a payment or savings account.
Directive (EU) 2019/882	Directive on accessibility requirements for products and services.	The directive sets out accessibility obligations for people with disabilities/impairments. Banking and financial services include payment account services and clearly refers to PSD2 for payment services and to the PAD directive for payment accounts.
Directive (EU) 2019/1153	Directive laying down rules to facilitate the use of financial and other information for the prevention or detection of certain criminal offences.	The Directive refers to the concept of payment account from the defined term "bank account information", which provides that the identifier of a payment account is the IBAN, which is also the identifier provided for in the central registers (see Article 32a of Directive 2015/849).
Directive (EU) 2016/97	Directive on the distribution of insurance.	This directive concerns the rules applicable to intermediaries and, in particular, ancillary insurance products and covers the hypothesis of insurance products ancillary to "payment accounts" as defined in the PAD (cross-selling) directive.
Regulation (EU) 2017/2394	Regulation on cooperation between national authorities responsible for	It aims to protect consumers and applies in addition to the provisions for consumers concerning payment accounts set out in the PAD directive.

	the enforcement of consumer protection laws.	The Regulation does not contain any further details, but recital 49 states that it is intended to apply in addition to the provisions "*concerning the protection of the collective economic interests of consumers in the area of payment account services*".
Regulation (EU) 2022/868	Regulation on European data governance.	The regulation refers to the need to apply no discrimination according to the location of the payment account by public entities.
Directive (EU) 2019/1937	Directive on the protection of persons who report breaches of Union law.	The directive aims to protect people who report breaches of EU law, particularly as regards provisions applicable to consumers, and by reference in Annex I, Part I, point ix), refers to the provisions applicable to consumers in the PAD directive.
Directive (EU) 2020/1828	Directive on representative actions to protect the collective interests of consumers.	The Directive lists the provisions of EU law which may be the subject of representative action in the event of an infringement by a professional. The PAD is referred to in Annex I of the Directive and is therefore a reference directive on payment accounts. The directive also covers PSD2.
Delegated Regulation (EU) 2018/32	Regulation defining the standardised terminology adopted at EU level for the most representative services attached to a payment account.	This is a regulation implementing the PAD directive (L2).
Implementing Regulation (EU) 2019/410	Regulation laying down implementing technical standards concerning the details and structure of the information to be notified by competent authorities to the	This is a regulation implementing the PSD2 Directive (L2).

	European Banking Authority in the field of payment services.	
Delegated Regulation (EU) 2021/1722	Regulation defining technical regulatory standards specifying the framework for cooperation and exchange of information between competent authorities.	This is a regulation implementing the PSD2 Directive (L2).
Delegated Regulation (EU) 2017/2055	Regulation laying down technical regulatory standards relating to cooperation and the exchange of information between competent authorities in connection with the exercise of the right of establishment.	This is a regulation implementing the PSD2 Directive (L2).
Regulation (EU) 2020/2011	Regulation on payment statistics.	The Regulation defines the nomenclature applicable to the statistics that the payment service providers provided for in the PSD2 Directive must supply to the competent authorities. With regard to the concept of payment account, this regulation refers to the concept of payment account provided for in the PSD2 (article 4 paragraph 12).

APPENDIX VII – COURT RULINGS ON THE LIABILITY OF THE ASPSP VIS-À-VIS THE CUSTOMER

1. Tribunal de commerce de Saint Nazaire, 15 juin 2022, affaire n° 2021001463

Affaire n°:2021001463
Jugement en date du 15/06/2022

GREFFE DU TRIBUNAL DE COMMERCE DE SAINT-NAZAIRE
Cour d'Appel de Rennes

EXTRAIT DES MINUTES DU GREFFE

JUGEMENT ENTRE

Monsieur

et:

SA

COPIE EXECUTOIRE DE JUGEMENT
en 1 pages

2022 000295

TRIBUNAL DE COMMERCE DE SAINT NAZAIRE
(Cour d'Appel de Rennes)

RG : 2021001463

DATE : 15 juin 2022

JUGEMENT PRONONCE PAR MISE A DISPOSITION AU GREFFE.

COPIE EXECUTOIRE DELIVREE
LE 15/06/2022
à Me GOSSELIN

COMPOSITION DU TRIBUNAL LORS DES DEBATS ET DU DELIBERE :

PRESIDENT : Madame Patricia RETAILLEAU
JUGES : Monsieur Dominique DURAND
Monsieur Olivier GUILLAUME

GREFFIER LORS DES DEBATS ET DU PRONONCE DU JUGEMENT : Monsieur Sébastien MASMEJEAN

DATE DES DEBATS : 13 avril 2022

PARTIES EN CAUSE :

DEMANDEURS :

Monsieur , né le , de nationalité , domicilié

Madame , née le , de nationalité çaise, domiciliée

Ayant pour Avocat La SELARL CARCREFF CONTENTIEUX D'AFFAIRES, représentée par Maître Cristina CORGAS, Avocate au barreau de Rennes.

DEFENDERESSE

SOCIÉTÉ GÉNÉRALE, SA dont le siège est situé 29, boulevard Haussmann 73009 PARIS, immatriculée au registre de commerce et des sociétés de Paris B sous le numéro 552 120 222 agissant poursuites et diligences de ses représentants légaux domiciliés en cette qualité audit siège.

Ayant pour Avocat la SCP Cabinet GOSSELIN, Maître GOSSELIN, avocat au barreau de RENNES.

FAITS

Monsieur et Madame ont ouvert auprès de l'agence SOCIETE GENERALE de deux comptes bancaires identifiés sous les numéros pour Monsieur et pour Madame.
Du 22 au 25 novembre 2020, 6 opérations débitrices étaient effectuées sur ces deux comptes, pour un montant global de 24 131,45 €.
Le 26 novembre 2020, Monsieur et Madame signalaient formellement à l'agence SOCIETE GENERALE de le caractère non autorisé de ces opérations et, par l'intermédiaire de leur conseillère bancaire, adressaient alors une demande de remboursement auprès de la SOCIETE GENERALE.

PR 1/7

Le 7 décembre 2020, le Service Cartes de la SOCIETE GENERALE notifiait aux époux son refus de remboursement puisque c'était bien leurs cartes qui avaient été utilisées.
Le 27 janvier 2021, le Conseil de Monsieur et Madame rappelait à la SOCIETE GENERALE, les manquements à son obligation de vigilance, et la mettait en demeure, d'avoir à régler la somme de 24 131,45 €.
La SOCIETE GENERALE ne répondant pas à cette mise en demeure, Monsieur et Madame ont saisi la présente juridiction.

PROCEDURE

C'est dans ce contexte que, suivant acte en date du 20 avril 2021, l'assignation a été signifiée en personne, à Madame , Directrice d'Agence, par Maître DAHAN huissier de justice.
L'affaire a fait l'objet de quatre renvois en mise en état, à la demande des parties.
Le 23 novembre 2021, puis le 24 février 2022, le conseil de Monsieur et Madame ont déposé leurs conclusions
Le 17 septembre 2021, puis le 29 décembre 2021 et le 31 mars 2022, le conseil de la SOCIETE GENERALE a déposé ses conclusions.
L'affaire étant en état d'être plaidée, les parties ont été régulièrement convoquées le 13 avril 2022, devant le Tribunal pour être entendues en leurs explications.
Elles se sont toutes présentées et ont été entendues.
Au cours de son audience publique du même jour, et après avoir entendu les parties, le Tribunal a prononcé la clôture des débats, a mis l'affaire en délibéré au 15 juin 2022 et précisé aux parties que le jugement sera rendu par disposition au greffe.

PRETENTIONS DES PARTIES

Par conclusions numéro 2 du 13 avril 2022, Monsieur et Madame demandent au Tribunal de :
Vu les articles L. 133-6, L. 133-18 et suivants du Code monétaire et financier,
Vu l'article 1231-1 du Code civil,
Vu la jurisprudence et les pièces versées au débat,
A TITRE PRINCIPAL,

- CONSTATER le caractère non autorisé des opérations bancaires signalées par les époux pour un montant global de 24 131,45 €
- CONSTATER que la SOCIETE GENERALE ne justifie pas des pouvoirs contractuels l'autorisant à procéder aux opérations frauduleuses ;
- CONSTATER l'absence d'un mécanisme d'authentification forte préalable aux opérations bancaires non autorisées ;

En conséquence,
- CONDAMNER la SOCIETE GENERALE à verser aux époux la somme de 24 131,45 € au titre de son obligation de remboursement des opérations non autorisées.

A TITRE SUBSIDIAIRE,
- DIRE ET JUGER que la SOCIETE GENERALE a manqué à son obligation de vigilance causant à Monsieur et Madame un préjudice financier,
- DIRE ET JUGER que la SOCIETE GENERALE a également manqué à ses obligations contractuelles tenant aux plafonds autorisés, ainsi qu'à son obligation d'information et d'alerte ;

En conséquence,
- CONDAMNER la SOCIETE GENERALE à verser aux époux la somme de 24 131,45 € au titre de l'indemnisation de leur préjudice ;

En tout état de cause,
- CONDAMNER la SOCIETE GENERALE à verser aux époux la somme de 3 000 € au titre de l'article 700 du Code de procédure civile ;

- CONDAMNER la SOCIETE GENERALE aux entiers dépens.

Par conclusions numéro 4 du 13 avril 2022, la SOCIETE GENERALE demande au Tribunal de :

Vu l'article 4 du code de procédure civile.
Vu d'article 1353 du Code civil
Déclarer les requérants irrecevables et subsidiairement mal fondés en leur chef tendant à «constater » que Société Générale ne justifierait pas des pouvoirs contractuels l'autorisant à procéder aux opérations frauduleuses.
Les déclarer irrecevables et les débouter en tant que, inversant la charge de la preuve, ils se soustraient à la communication des pièces contractuelles dans le cadre de leur action en responsabilité contractuelle,
Débouter Monsieur et Madame de l'ensemble de leurs demandes, fins et conclusions fondées sur un manquement à l'absence d'autorisation des opérations et aux mécanismes d'authentification.
Les débouter de leur demande au titre d'une obligation de remboursement d'opérations prétendument non autorisées, quel qu'en soit le fondement.
Sur la demande subsidiaire.
Débouter Monsieur et Madame de l'ensemble de leurs demandes, fins et conclusions fondées sur un manquement à l'obligation de vigilance, où à un prétendu manquement à une obligation d'information et d'alerte.
En toutes hypothèses,
Les débouter de toutes demandes, fins et conclusions.
Les condamner *in solidum*, au paiement d'une somme de 3 000 € au titre de l'article 700 du code de procédure civile et aux entiers dépens,
Subsidiairement
Les débouter de toutes demandes d'exécution provisoire

MOYENS DES PARTIES

Monsieur et Madame exposent (en synthèse de 16 pages de conclusions, appuyées de 9 pièces) :

A TITRE PRINCIPAL SUR L'OBLIGATION DE REMBOURSEMENT DE LA SOCIETE GENERALE

1. L'absence de preuve des pouvoirs de la SOCIETE GENERALE

Monsieur et Madame disposent de deux comptes ouverts à la SOCIETE GENERALE, l'un au nom de Madame , l'autre au nom de Monsieur .
Les opérations frauduleuses ont été réalisées sur chacun de ces comptes, par l'intermédiaire de codes uniques.
La banque devra justifier que le système d'authentification utilisé par Monsieur l'autorisait à procéder aux opérations sur chacun des comptes. Elle devra pour ce faire, produire les contrats qui la lie aux demandeurs et plus précisément le mandat que Madame a donné à Monsieur pour que celui-ci puisse disposer de son compte bancaire, Madame soutenant qu'un tel mandat est inexistant.

2. Le caractère non autorisé des opérations signalées par les époux et l'obligation de remboursement de la SOCIETE GENERALE

- A leurs montants et à la nature des opérations

*Sur le compte de Monsieur sur lequel ont été faits deux achats à LEROY MERLIN et les virements au profit de : ce compte connaît essentiellement des opérations de prélèvements et des achats surtout de nature alimentaire ; le montant des achats n'atteint jamais les montants détournés.

*Sur le compte de Madame : ce compte ne connaît que de rares débits pour des montants modestes ; l'achat de Leroy Merlin de 5 646,17 euros est parfaitement anormal.

- A leur succession dans le temps

Pas moins de six opérations en trois jours ont été réalisées sur le compte des demandeurs pour des sommes significatives, ce qui est parfaitement inhabituel sur le compte de Monsieur et l'est davantage sur celui de Madame .

- A la plainte et à l'enquête consécutive

Les époux ont immédiatement porté plainte dès qu'ils ont découverts la fraude dont ils ont été victimes.

La SOCIETE GENERALE réplique (en synthèse de 15 pages de conclusions, appuyées de 5 pièces)

A) Sur l'obligation de remboursement

Les requérants sont mal fondés à se prévaloir d'une prétendue absence de preuve de pouvoirs de la Société Générale alors que, demandeurs, ils sont débiteurs de l'obligation probatoire, en application de l'article 1353 du code civil et savent mieux que quiconque s'ils ont l'un ou l'autre donné pouvoir à l'un et l'autre, et ce d'autant qu'ils plaident ensemble sous la même constitution.

A.1/ Sur la négligence des époux

Il résulte de l'article L 133.19 du code monétaire et financier que

« (...) IV – Le payeur supporte toutes les pertes occasionnées par des opération de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux article L 133-16 et L 133-17. »

Il appartient à l'utilisateur de services de paiement de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et d'informer sans tarder la banque de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées,

Le site internet de SOCIETE GENERALE particuliers dispense à ses clients des conseils liés à la sécurité et la vigilance face au phishing et à l'utilisation de l'EIP (Espace Internet Particuliers).

Monsieur a délibérément transmis par téléphone des données strictement personnelles se rapportant au dispositif de sécurité personnalisé associé à ses services de paiement.

Ce comportement constitue une négligence grave excluant tout droit à indemnisation.

Les faits démontrent que Monsieur connaissait les identifiants personnels de son épouse, qu'elle lui avait vraisemblablement communiqués par négligence.

A.2/ sur l'authentification forte

Il résulte de l'article L. 133-44 du code monétaire et financier que l'authentification forte ne doit être appliquée que dans trois hypothèses :

- Lorsque le payeur accède à son compte de paiement en ligne ;
- Lorsqu'il initie une opération de paiement électronique ;
- Lorsqu'il désigne une opération par le biais d'un moyen de communication à distance susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

Il résulte des déclarations de Monsieur que des numéros de code lui ont été envoyés sur son téléphone portable aux fins de validation des opérations litigieuses et qu'il a délibérément transmis par téléphone à un tiers dont il ignorait l'identité.

B./ Subsidiairement sur l'obligation de vigilance

B.1/ Sur l'absence d'anomalie apparente

Le devoir de vigilance doit s'exercer dans le respect de l'obligation de non-ingérence.

L'anomalie apparente est celle qui ne doit pas échapper au banquier suffisamment prudent et diligent face à des faits anormaux et manifestement litigieux.

La banque manque à son devoir de vigilance en exécutant un ordre de virement anormal. Or, les virements réalisés en la circonstance, d'un montant individuel inférieur à 4 000 €, ne présentaient pas de caractère particulièrement disproportionné au regard du fonctionnement de leur compte et de leur situation financière.

La responsabilité délictuelle de SOCIETE GENERALE n'est pas engagée et la demande sera rejetée.

B.2/ Sur les plafonds de virement

Les requérants prétendent que les virements auraient dû être bloqués automatiquement au motif qu'ils ne sauraient excéder 7 623 € par jour ouvré.

Or, ils ne font état que de 3 virements litigieux, chacun d'un montant de 4 000 €, effectués les 23,24 et 25 novembre 2020 depuis le compte bancaire de Monsieur .

Les plafonds des virements initiés à distance par le biais de l'application ou de l'EIP sur un ordinateur sont plafonnés à 4 000 € par jour,

Les autres opérations litigieuses ne sont pas des virements mais des paiements par carte bancaire, non concernés par les plafonds applicables aux virements.

B.3/ Sur l'alerte

La SOCIETE GENERALE diffuse sur son site internet des conseils liés à la sécurité et la vigilance face au phishing et à l'utilisation de l'EIP et les agences diffusent régulièrement des messages vocaux de prévention via leur temps d'attente téléphonique.

SUR QUOI, LE TRIBUNAL,

Sur la demande principale

Vu les articles L. 133-6, L. 133-18 et suivants du Code monétaire et financier,
Vu l'article 1231-1 du Code civil,

Attendu que l'article L. 133-6 du code monétaire et financier est libellé :

« I. – Une opération de paiement est autorisée si le payeur a donné son consentement à son exécution.

Toutefois, le payeur et son prestataire de services de paiement peuvent convenir que le payeur pourra donner son consentement à l'opération de paiement après l'exécution de cette dernière.

II. – Une série d'opérations de paiement est autorisée si le payeur a donné son consentement à l'exécution de la série d'opérations, notamment sous la forme d'un mandat de prélèvement. »

Qu'en l'espèce, les payeurs sont Monsieur et Madame au regard dudit article ;

Qu'en l'occurrence, à la lecture du compte-rendu d'infraction initial PV n° 00279/2020/002628, du 27 novembre 2020, Monsieur confirme avoir donné de son plein gré, par téléphone ses numéros de compte, de cartes bancaires, pour lui et son épouse, leurs identifiants ;

Qu'il y confirme également, avoir transmis à son interlocuteur, les codes de validation reçus sur son téléphone ;

Que dès lors, leur consentement mutuel a été donné sur une procédure de vérification qui leur était connue ;

Qu'il importe peu de savoir si Madame avait donné mandat à son époux Monsieur puisque le même compte-rendu indique que Madame était présente lors de l'appel téléphonique, a elle-même téléphoné au commissariat de , en a fait part à son époux et donc, a consenti à la divulgation de ses données personnelles ;

Que les opérations ont été parfaitement autorisées par les payeurs ;

Que toujours déclaré par Monsieur auprès de l'officier de police le 27 novembre 2020, « *Hier, j'ai été alerté par mon conseiller de la banque SOCIETE GENERALE de qu'il y avait des mouvements inhabituels sur nos comptes bancaires dont le n° IBAN est : en ce qui me concerne et pour celui de mon épouse* » ;

Que par cette déclaration, la banque SOCIETE GENERALE en ayant prévenu Monsieur et Madame , le 26 novembre 2020, alors que ces derniers n'avaient pas vérifié leurs comptes, a démontré une attention particulière à avertir ses clients ;

Qu'il ne peut donc pas être reproché à la SOCIETE GENERALE d'avoir manqué à ses obligations de vigilance, d'information et d'alerte ;

En conséquence, le tribunal déboutera Monsieur et Madame de leurs toutes leurs demandes, fins et conclusions, vis-à-vis de la SOCIETE GENERALE ;

Sur l'article 700 du CPC

Attendu qu'il serait inéquitable de laisser à la charge de la SOCIETE GENERALE, la totalité des frais irrépétibles qu'elle a dû exposer pour faire valoir ses droits en justice ;

Qu'en conséquence, Monsieur et Madame seront condamnés *in solidum* à lui payer la somme de 1 500 € au titre de l'article 700 du CPC à la SOCIETE GENERALE ; que le tribunal déboutera cette dernière du surplus de sa demande ;

Sur les dépens

Attendu que les entiers dépens de la présente instance seront mis à la charge in solidum de Monsieur et Madame qui succomberont en l'instance ;

PAR CES MOTIFS :

Après en avoir délibéré, le Tribunal statuant par jugement public contradictoire en premier ressort

DEBOUTE Monsieur et Madame de leurs toutes leurs demandes, fins et conclusions, vis-à-vis de la SOCIETE GENERALE.

CONDAMNE in solidum Monsieur et Madame à payer à la SOCIETE GENERALE la somme de 1 500 € au titre de l'article 700 du CPC et DEBOUTE la SOCIETE GENERALE du surplus de sa demande au titre de l'article 700 du CPC.

CONDAMNE in solidum Monsieur et Madame aux entiers dépens de l'instance.

LIQUIDE les frais de greffe à la somme de 80,29 € dont TVA 13,38 €.

La minute du jugement est signée par Madame Patricia RETAILLEAU, Président, et par Monsieur Sébastien MASMEJEAN, Greffier.

Tribunal de commerce de Saint-Nazaire

N° RG : 2021001463
Jugement du 15/06/2022
1 - CONTENTIEUX GENERAL Audience publique - plaidoiries

En conséquence, la République Française mande et ordonne à tous Huissiers de justice, sur ce requis, de mettre ladite décision à exécution, aux Procureurs Généraux et aux Procureurs de la République près les Tribunaux judiciaires d'y tenir la main, à tous Commandants et Officiers de la force publique, de prêter main-forte, lorsqu'ils en seront légalement requis.

Pour expédition certifiée conforme
et revêtue de la formule exécutoire.

Expédition délivrée le 15/06/2022

Le Greffier,

2. Tribunal judiciaire de Paris, 8 juin 2022, 9eme chambre 2ème section, n° RG 19/04840

TRIBUNAL JUDICIAIRE DE PARIS

■

9ème chambre
2ème section

N° RG 19/04840
N° Portalis
352J-W-B7D-CPV5
M

N° MINUTE : 5

JUGEMENT
rendu le 08 Juin 2022

Assignation du :
08 Avril 2019

DEMANDERESSE

Madame

représentée par Maître Emma BENSOUSSAN CREMIEUX de la SELARL VESPERA AVOCATS, avocats au barreau de PARIS, avocats postulant, vestiaire #G0177

DÉFENDERESSE

S.A. BNP PARIBAS
16 Boulevard des Italiens
75009 PARIS

représentée par Maître Nicolas BAUCH-LABESSE de l'AARPI TARDIEU GALTIER LAURENT DARMON associés, avocats au barreau de PARIS, avocats postulant, vestiaire #R0010

Expéditions exécutoires délivrées le:

COMPOSITION DU TRIBUNAL

Monsieur Gilles MALFRE, 1er Vice-président adjoint
Madame Marie-Albanie TERRIER, Vice-présidente
Monsieur Augustin BOUJEKA, Vice-Président

assistés de Clarisse GUILLAUME, Greffier,

DÉBATS

A l'audience du 13 Avril 2022 tenue en audience publique devant Madame TERRIER, juge rapporteur, qui, sans opposition des avocats, a tenu seule l'audience, et, après avoir entendu les conseils des parties, en a rendu compte au Tribunal, conformément aux dispositions de l'article 805 du Code de Procédure Civile. Avis a été donné aux conseils des parties que la décision serait rendue par mise à disposition au greffe le 8 juin 2022.

JUGEMENT

rendu publiquement par mise à disposition
contradictoire
en premier ressort

EXPOSE DU LITIGE

Madame est titulaire d'un compte-courant n° et d'un livret A n° ouverts dans les livres de BNP PARIBAS.

Au mois de juillet 2018, des opérations ont été réalisées sur son compte:

- deux nouveaux bénéficiaires de virement ont été ajoutés à la liste établie en ligne ;
- deux transferts d'argent ont été effectués à partir de son compte épargne vers son compte courant ;
- deux virements ont été effectués à partir de son compte courant vers l'étranger au profit de bénéficiaires :
  - un premier virement de 9.866 € a été réalisé, le 28 juillet 2018, au bénéfice de «Madame »;
  - un second virement de 5.201 € a été réalisé, le 31 juillet 2018, au bénéfice de « »;
- un débit a été effectué sur sa carte bancaire pour un montant de 2.604,82 € au profit de la société , soit un montant total de 17.671,82 euros.

S'estimant victime d'un piratage de ses données bancaires, et soutenant ne pas être à l'origine de ces opérations, ni ne connaître les bénéficiaires des virements, Madame a signalé ces opérations auprès de BNP Paribas en :

- les dénonçant au directeur de son agence par courriers en date des 31 juillet et 3 août 2018;
- en remplissant et retournant à BNP Paribas, le 7 août 2018, les formulaires de contestation d'opération d'usage confirmant l'absence d'autorisation de sa part tant pour les deux virements en ligne que pour le paiement effectué avec sa carte bancaire et en faisant opposition à sa carte bancaire.

La BNP Paribas a refusé de l'indemniser de ces opérations au motif qu'elles ont été confirmées et authentifiées par sa cliente.

Par exploit d'huissier en date du 8 avril 2019, Mme l'a faite assigner devant la présente juridiction pour faire reconnaître l'existence d'une fraude de type « *hacking* » sur ses comptes bancaires et condamner la banque à prendre en charge le montant des opérations contestées.

Aux termes de ses dernières écritures, notifiées le 23 février 2021, Mme demande au tribunal, sur le fondement des articles L.133-18, L.133-23, L. 133-24, et L. 561-10-2 du code monétaire et financier, de:
- condamner la SA BNP Paribas à lui restituer la somme de 17.671,82 € en principal indûment débitée se décomposant comme suit :

• 9.866 € en remboursement du virement frauduleux effectué le 28 juillet 2018 au bénéfice de « » ;
• 5.201 € en remboursement du virement frauduleux effectué le 31 juillet 2018 au bénéfice de « » ;
• 2.604,82 € en remboursement du paiement frauduleux du 31 juillet 2018 effectué via sa carte bancaire ;

- condamner la banque BNP Paribas à lui payer sur cette somme les intérêts de retard dus à compter de la délivrance de l'assignation ;
- ordonner la capitalisation des intérêts ;
- condamner la BNP Paribas au paiement de la somme de 3.000 € à titre de dommages et intérêts pour résistance abusive résultant du refus abusif à lui rembourser les sommes dues ;
- condamner la BNP Paribas au paiement de la somme de 5.000 € à titre de dommages et intérêts au titre du préjudice moral subi par Madame ;
- condamner la BNP Paribas à lui payer la somme de 5.000 € sur le fondement de l'article 700 du code de procédure civile ;
- condamner la BNP Paribas aux entiers dépens dont distraction au profit de la Selarl Vespera Avocats ;
- ordonner l'exécution provisoire du jugement à intervenir.

Par conclusions en défense, signifiées le 15 juin 2021, la BNP Paribas demande au tribunal, sur le fondement des dispositions de l'article 10 du code civil, des articles L. 133-16 et suivants du code monétaire et financier, l'article 1240 du code civil (ancien 1382 du même code), de l'article 1147 du code civil, et les articles L. 561-1 et suivants du code monétaire et financier, de débouter Mme de ses demandes et la condamner au paiement d'une somme de 5000 euros au titre de l'article 700 du code de procédure civile, outre les dépens.

L'ordonnance de clôture est intervenue le 1er septembre 2021, et l'affaire a été évoquée à l'audience du 13 avril 2022.

MOTIFS DE LA DÉCISION

Mme soutient que la SA BNP Paribas est débitrice d'une obligation de remboursement, et ce même en cas d'utilisation de l'instrument de paiement, en application des articles L.133-18 et L.133-23 du code monétaire et financier. Elle prétend qu'il ne peut lui être reproché aucune négligence fautive, ni fraude, la SA BNP Paribas étant défaillante à rapporter cette preuve. Elle estime que la BNP Paribas a manqué à son devoir de diligence et se prévaut d'une part de l'article 1147 du code civil et d'autre part, du devoir de vigilance spécial, prévu aux articles L. 561-1 et suivants du code monétaire et financier concernant les règles relatives à la lutte contre le blanchiment et le financement du terrorisme.

La banque soutient que Mme ne rapporte pas la preuve de la fraude dont elle se plaint, en se contentant de soutenir que les opérations sont le résultat d'un *"hacking"*, sans pour autant avoir pris la peine de déposer une plainte ou de se rendre au rendez-vous donné par son agence bancaire pour traiter de ces demandes en remboursement. Elle relève que les opérations contestées par la demanderesse ont bien été authentifiées, enregistrées et comptabilisées sans qu'il ne soit fait état de la moindre défaillance technique, les virements litigieux ayant été réalisés par l'intermédiaire de sa clé digitale, laquelle relève de l'authentification forte, le paiement en ligne ayant été autorisé par l'envoi d'un code par SMS sur son téléphone portable.

Elle estime inconcevable que l'ensemble des informations confidentielles de Mme aient été en possession d'un tiers, sans qu'aucune faute ou négligence de sa cliente ne puisse en être à l'origine. S'agissant de son devoir de vigilance, elle rappelle que sa cliente ne peut pas lui opposer les dispositions relatives au blanchiment, et qu'elle est tenue au contraire d'un devoir de non immixtion dans les affaires de son client.

L'article L. 133-18 du code monétaire et financier dispose que *« En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L 133-24, le prestataire de services de paiement du payeur rembourse au payeur le montant de l'opération non autorisée immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, sauf s'il a de bonnes raisons de soupçonner une fraude de l'utilisateur du service de paiement et s'il communique ces raisons par écrit à la Banque de France. Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu.*
Lorsque l'opération de paiement non autorisée est initiée par l'intermédiaire d'un prestataire de services de paiement fournissant un service d'initiation de paiement, le prestataire de services de paiement gestionnaire du compte rembourse immédiatement, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. La date de valeur à laquelle

le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il avait été débité.
Si le prestataire de services de paiement qui a fourni le service d'initiation de paiement est responsable de l'opération de paiement non autorisée, il indemnise immédiatement le prestataire de services de paiement gestionnaire du compte, à sa demande, pour les pertes subies ou les sommes payées en raison du remboursement du payeur, y compris le montant de l'opération de paiement non autorisée.
Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire ».

Il est dit aux IV et V de l'article L. 133-19 du code monétaire et financier, que "*Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133-17.*
Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une authentification forte du payeur prévue à l'article L. 133-44."

L'article L. 133-23 du même code dispose que "*Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.*
L'utilisation de l'instrument de paiement telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière. Le prestataire de services de paiement, y compris, le cas échéant, le prestataire de services de paiement fournissant un service d'initiation de paiement, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement."

Il est acquis qu'en application de ces textes, le teneur de compte est tenu de rapporter la preuve d'une négligence grave dans la conservation des données de sécurité par le titulaire du compte pour s'exonérer de cette responsabilité de plein droit.

Au cas présent, il n'est pas contesté que les deux virements, dont les noms des bénéficiaires étaient Mme et le syndicat des copropriétaires du , ont été authentifiés suivant le système de clé digitale, permettant d'authentifier les demandes de paiement du titulaire du compte, de désignation de nouveaux bénéficiaires de virements, et de virements à des tiers en entrant un code secret (clé digitale) depuis son seul téléphone portable,

suivant un service qui n'a pu être mis en place qu'avec l'apposition de son empreinte digitale.

Ainsi, une fois la clé digitale enregistrée, la validation des opérations susvisées doit obligatoirement être effectuée au moyen de cette clé, et ce depuis le terminal mobile sur lequel la clé a été installée. Il s'agit donc d'une authentification forte au sens de l'article L. 133-4 f) et du V de l'article L. 133-19 du code monétaire et financier.

Dans ce cadre, et dès lors que la demanderesse ne fait pas état du vol de son téléphone portable, il ne peut qu'être considéré que les opérations ont été effectuées depuis celui-ci, et approuvées par la personne non seulement en possession de son téléphone, mais également ayant connaissance de sa clé digitale. Il doit en être déduit que ces virements ont nécessairement été authentifiés par elle, ou par une personne qui avait à sa disposition ces éléments personnels et secrets de Mme .

Le seul fait que la demanderesse affirme ne pas connaître et la production du relevé du compte de gestion de son syndicat de copropriété, lequel est d'ailleurs désigné comme étant bien le " ", ne mentionnant pas en crédit le virement en cause, ne démontrent pas l'absence d'autorisation émanant de la demanderesse, ni même l'absence d'encaissement effectif de cette somme par le syndicat de copropriété, la pièce versée n'étant pas exhaustive. Enfin, il n'est fait état d'aucune faille dans le système de sécurité de paiement.

S'agissant du paiement en ligne au profit de la société , la banque démontre avoir envoyé un SMS de confirmation de paiement au numéro de téléphone attribué à Mme , sans que celle-ci conteste l'attribution de ce numéro de téléphone. Or, sans l'apposition de ce code dont seule la personne en possession de son téléphone a connaissance, le paiement en ligne n'a pas pu être effectué. Par conséquent, il doit en être déduit à l'identique que Mme a authentifié ce paiement, ou laissé son téléphone personnel à la disposition d'un tiers par négligence.

S'agissant du défaut de vigilance, il convient tout d'abord de rappeler que les dispositions du code monétaire et financier relatives à la lutte contre le blanchiment ne peuvent pas être invoquées par un particulier.

Par ailleurs, il y a lieu de rappeler que selon le principe de non-immixtion, il est constant que le banquier n'a pas à se substituer à son client dans la conduite de ses affaires, ni à intervenir pour empêcher son client d'effectuer un acte irrégulier, inopportun ou dangereux.

En outre, la banque n'a pas à effectuer de recherches, à réclamer de justifications pour s'assurer que les opérations qui lui sont demandées par un client sont régulières. Toutefois ce principe cède en présence d'anomalies et d'irrégularités manifestes, que le banquier doit détecter.

Pour le banquier, non alerté par des éléments extérieurs tangibles, le simple caractère inhabituel d'une opération n'implique pas nécessairement qu'elle soit illicite ou frauduleuse.

Au cas présent, le tribunal n'est tout d'abord pas mis en mesure d'apprécier le caractère anormal de ces opérations alors qu'il n'est produit qu'un extrait du relevé du compte chèques de Mme portant sur son fonctionnement durant un mois. Mais surtout, le compte chèque de Mme a été préalablement alimenté par son livret A, avant de réaliser les opérations dont elle conteste être l'auteur, de sorte que la banque n'a pu que penser qu'elle était l'auteur de ces paiements ou virements. Dans ces conditions, alors que les opérations n'apparaissent pas anormales, il ne saurait être reproché à la banque, tenue d'un devoir de non-ingérence dans les affaires de sa cliente, de ne pas s'être rapprochée d'elle afin de vérifier l'authenticité des ordres de paiement.

Dans ces conditions, Mme n'apparaît pas fondée dans ses demandes.

La banque n'étant pas tenue au remboursement des sommes réclamées par Mme , et ne voyant aucune faute pouvant lui être reprochée, la demanderesse sera également déboutée de ses prétentions formées au titre de la résistance abusive, ou en réparation de son préjudice moral.

Dans la mesure où elle succombe, Mme sera condamnée aux entiers dépens.

L'équité commande de la condamner au paiement d'une indemnité d'un montant de 1500 euros au titre de l'article 700 du code de procédure civile au profit de la banque.

La solution apportée au présent litige rend sans objet la demande d'exécution provisoire.

PAR CES MOTIFS

Le tribunal, statuant par jugement contradictoire, rendu en premier ressort, publiquement, par mise à disposition au greffe

Déboute Mme de l'ensemble de ses demandes,

La condamne au paiement à la SA BNP Paribas d'une somme de 1500 euros au titre de l'article 700 du code de procédure civile,

La condamne aux entiers dépens,

Dit n'y avoir lieu au prononcé de l'exécution provisoire.

Fait et jugé à Paris le 08 Juin 2022

Le Greffier Le Président

3. Tribunal judiciaire de Paris, 15 novembre 2022, n° RG 22/02540

TRIBUNAL JUDICIAIRE DE PARIS
Pôle civil de proximité
[redacted]

PCP JTJ proxi requêtes

N° RG 22/02540 - N° Portalis 352J-W-B7G-CWXU2

N° MINUTE :
2022/3

Extraits des minutes du greffe du tribunal judiciaire de Paris

République française,
Au nom du peuple français

JUGEMENT
rendu le mardi 15 novembre 2022

DEMANDEURS
Mxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxx
Assiqté par Me Avocate au Barreau de Paris
(Toque)

Mme xxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxx

représentée par Me Avocate au Barreau de Paris (Toque

DÉFENDERESSE
Société CAISSE REGIONALE DU CREDIT AGRICOLE MUTUEL DE PARIS ILDE DE FRANCE
26 quai de la Râpée
75012 PARIS
représentée par Me
Avocate au Barreau de Paris
(Toque)

COMPOSITION DU TRIBUNAL
Jean-Claude KAZUBEK, Juge, statuant en juge unique
assisté de Philippe PUEL, Greffier,

DATE DES DÉBATS
Audience publique du 07 octobre 2022

Copie conforme délivrée
le : 16 NOV 2022
à : demandeurs et défendeur

Copie exécutoire délivrée
le :
à :

Page 1

JUGEMENT
contradictoire, en dernier ressort, prononcé par mise à disposition le 15 novembre 2022 par Jean-Claude KAZUBEK, Juge assisté de Philippe PUEL, Greffier

Vu la requête reçue le 14 avril 2022 aux termes de laquelle Mxxxxxx et Madame xxxxx ont revendiqué, avec exécution provisoire, la condamnation de la CAISSE REGIONALE DU CREDIT AGRICOLE DE PARIS ILE DE FRANCE à lui payer les sommes suivantes :

- 1549 € correspondant à la transaction frauduleuse réalisée sur le compte bancaire joint numéro le 20 mai 2021, avec intérêts au taux légal à compter de la date de la tentative de conciliation du 24 novembre 2021

- 1000 € au titre de l'article 700 du code de procédure civile.

Vu les conclusions de la CAISSE REGIONALE DU CREDIT AGRICOLE DE PARIS ILE DE FRANCE tendant à voir :

- déclarer que l'opération de paiement électronique du 20 mai 2021 est une opération de paiement autorisée,

- débouter Mxxx et Madame xxx de l'intégralité de leurs demandes,

- condamner in solidum Mxxx et Madame xxxxx à lui payer la somme de 2500 € sur le fondement de l'article 700 du code de procédure civile,

- rappeler que l'exécution provisoire de la décision à intervenir est de droit.

Vu les dernières conclusions de Mxxx et Madame xxxxx s'opposant aux assertions de la défenderesse et réitérant les termes de leur requête initiale.

Vu les dossiers des parties et les documents qu'ils contiennent à l'attention de la juridiction.

Pour satisfaire aux prescriptions de l'article 455 du code de procédure civile, ce tribunal déclare se rapporter au contenu de ces actes et documents en ce qui concerne les prétentions respectives des parties et leurs moyens.

Vu les explications orales.

MOTIFS.

Il est constant que Mxx et Madame xx sont titulaires d'un compte joint de dépôt numéro xxxxx ouvert dans les livres de la CAISSE REGIONALE DU CREDIT AGRICOLE DE PARIS ILE DE FRANCE.

Mxxxx et Madame xxxxx font grief à la CAISSE REGIONALE DU CREDIT AGRICOLE DE PARIS ILE DE FRANCE d'avoir procédé à un paiement frauduleux de 1549 € effectué le 20 mai 2021 sur ce compte dont ils s'en sont aperçus le 29 mai suivant, procédant entre autre, un signalement ligne auprès des services de la gendarmerie nationale

Ils ajoutent que toutes démarches entreprises auprès de l'établissement bancaire sont demeurées infructueuses, nécessitant l'instauration de la présente procédure.

Les requérants ont contesté avoir autorisé l'opération litigieuse, soutenant notamment n'avoir commis aucune négligence.

Il résulte des dispositions de l'article L 133-6 du Code monétaire et financière qu'une opération de paiement est autorisée si le payeur a donné son consentement à son exécution, que l'article L 133-7 de ce même code précise que le consentement est donné sous la forme convenue entre le payeur et son prestataire de services de paiement.

L'article L 133 – 44 I 2° de ce même code ajoute que l'authentification forte est requise lorsqu'une banque initie une opération de paiement électronique.

En l'espèce, il n'apparaît pas sérieusement contestable que le 29 mars 2021 Mxxxx a souscrit au dispositif SECURIPASS, enrôlé à son téléphone mobile.

Il y a lieu de relever que la CAISSE REGIONALE DU CREDIT AGRICOLE DE PARIS ILE DE FRANCE a, au cours des débats, présenté, contradictoirement, une description exhaustive du fonctionnement du système SECURIPASS.

Mxxxx ne saurait valablement soutenir que l'adhésion à un tel service ne pourrait être interprétée comme une volonté propre du client utilisateur, dès lors qu'il n'y aurait aucune manœuvre concernant les modalités et conditions d'utilisation de services et qu'en pratique, il ne pourrait s'opposer à la souscription de ce service sans lequel il ne réaliser des achats en ligne ni accéder à son application de gestion des comptes étant donné qu'il appert que la souscription audit service n'est aucunement automatique et qu'en son absence toutes opérations bancaires peuvent normalement être effectuées

Il est constant que Mxxxx a indubitablement validé l'opération de paiement électronique de 1549 € au moyen de l'authentification forte réalisée avec le dispositif SECURIPASS précité depuis son téléphone mobile et que l'authentification forte a ainsi permis de vérifier l'identité du donneur d'ordre par la combinaison des critères de « connaissance » / « inhérence » et l'empreinte digitale de celui-ci.

Il s'ensuit que l'opération a été dûment autorisée par Mxxxx lequel a donné son consentement à l'exécution, que par voie de conséquence, il ne saurait prospérer en ses allégations infondées et il doit donc être débouté de l'intégralité de ses demandes.

Aucune considération tirée de l'équité ou de la situation économique des parties ne justifie de faire application des dispositions de l'article 700 du code de procédure civile ;

qu'il convient de débouter la CAISSE REGIONALE DU CREDIT AGRICOLE DE PARIS ILE DE FRANCE de sa demande d'indemnité de procédure.

Conformément à l'article 696 du code de procédure civile, Mxxxxxxx et Madame xxxx doivent être condamnés in solidum aux entiers dépens de la présente procédure

PAR CES MOTIFS.

Statuant, après débats publics, par jugement prononcé par mise à disposition, les parties en ayant été préalablement visées dans les conditions de l'article 450, du code de procédure civile, contradictoirement et en dernier ressort

Déboute Mxx et Madame xxxx de l'intégralité de leurs demandes.

Déboute la CAISSE REGIONALE DU CREDIT AGRICOLE DE PARIS ILE DE FRANCE de sa demande d'indemnité de procédure.

Condamne in solidum Mxxx et Madame xxxx aux ent iers dépens de la présente procédure.

Ainsi fait et jugé, le 15 Novembre 2022.

Le greffier, le juge,

Pour copie conforme délivrée
à [redacted] sur ...4 pages
Le directeur de greffe

Page 4

4. Cour d'appel de Versailles, 28 mars 2023, RG n°21/07299

COUR D'APPEL

DE

VERSAILLES

Code nac : 38Z

13e chambre

ARRET N°

CONTRADICTOIRE

DU 28 MARS 2023

N° RG 21/07299

N° Portalis DBV3-V-B7F-U4C4

AFFAIRE :

[Y] [U]

C/

S.A. BNP PARIBAS

Page 1 / 12

Décision déférée à la cour : Jugement rendu le 03 Novembre 2021 par le Tribunal de Commerce de PONTOISE

N° Chambre : 0

N° Section : 0

N° RG : 2020F00353

Expéditions exécutoires

Expéditions

Copies

délivrées le :

à :

Me Monique TARDY

Me Niels ROLF-PEDERSEN

TC PONTOISE

RÉPUBLIQUE FRANÇAISE

AU NOM DU PEUPLE FRANÇAIS

LE VINGT HUIT MARS DEUX MILLE VINGT TROIS,

La cour d'appel de Versailles a rendu l'arrêt suivant dans l'affaire entre :

Monsieur [Y] [U]

né le [Date naissance 3] 1959 à [Localité 6]

de nationalité Française

[Adresse 1]

[Localité 5]

Représentant : Me Monique TARDY de l'ASSOCIATION AVOCALYS, Postulant, avocat au barreau de VERSAILLES, vestiaire : 620 - N° du dossier 005134

Représentant : Me Sylvie NOACHOVITCH de la SELARL SELARL INTER BARREAUX SYLVIE NOACHOVITCH & ASSOCIE, Plaidant, avocat au barreau de PARIS, vestiaire : C1833

APPELANT

****

S.A. BNP PARIBAS

[Adresse 2]

[Localité 4]

Représentant : Me Niels ROLF-PEDERSEN, Postulant, avocat au barreau de VERSAILLES, vestiaire : 291

Représentant : Me Dominique PENIN du LLP KRAMER LEVIN NAFTALIS & FRANKEL LLP, Plaidant, avocat au barreau de PARIS, vestiaire : J008

INTIMEE

****

Composition de la cour :

En application des dispositions de l'article 805 du code de procédure civile, l'affaire a été débattue à l'audience publique du 13 Décembre 2022 les avocats des parties ne s'y étant pas opposés, devant Madame Marie-Andrée BAUMANN, Conseiller chargé du rapport.

Ce magistrat a rendu compte des plaidoiries dans le délibéré de la cour, composée de :

Madame Marie-Andrée BAUMANN, Conseiller,

Madame Delphine BONNET, Conseiller,

Madame Véronique MULLER, Magistrat honoraire,

Greffier, lors des débats : Madame Sabine NOLIN,

M. [Y] [U] est titulaire dans les livres de SA BNP Paribas d'un compte auquel il peut accéder via l'application mobile de BNP Paribas.

Le 31 mai 2019, M. [U] a constaté que plusieurs virements frauduleux pour un montant de 54 500 euros avaient été réalisés depuis son compte bancaire ; il a prévenu sa conseillère le jour même, étant précisé qu'un prélèvement de 5 000 euros a pu être recrédité sur son compte puis il a déposé plainte le 3 juin 2019.

Par courriel, transmis le 1er août 2019 au pôle 'relations clients' de la BNP Paribas, M. [U] a dressé un 'compte-rendu des faits du 29 mai 2019' en rappelant que dès l'ouverture de l'agence le 31 mai, il l'en avait informée.

Par lettre du 8 août 2019, la BNP Paribas, contestant que sa responsabilité puisse être engagée et soutenant que M. [U] avait 'commis des imprudences et négligences graves' lui a indiqué qu'il ne serait pas donné une suite favorable à sa demande de remboursement.

Par acte d'huissier en date du 12 août 2020, M. [U] a assigné la BNP Paribas devant le tribunal de commerce de Pontoise, lequel, par jugement contradictoire assorti de l'exécution provisoire du 3 novembre 2021, a :

- débouté M. [U] de sa demande en paiement de la somme de 54 500 euros ;

- débouté ce dernier de ses demandes de dommages et intérêts au titre du préjudice moral et de la résistance abusive ;

- débouté celui-ci de sa demande en paiement sur le fondement de l'article 700 du code de procédure civile ;

- condamné M. [U] à payer à la BNP Paribas la somme de 800 euros au titre de l'article 700 du code de procédure civile ;

- condamné M. [U] aux entiers dépens de l'instance.

Par déclaration en date du 8 décembre 2021, M. [U] a interjeté appel du jugement.

Dans ses dernières conclusions déposées au greffe et notifiées par RPVA le 6 octobre 2022, il demande à la cour de :

- le recevoir en son appel et ses conclusions et l'y déclarer bien fondé ;

- infirmer le jugement en toutes ses dispositions ;

En conséquence, statuant de nouveau,

- condamner la BNP Paribas à lui payer la somme de 54 500 euros au titre du remboursement des fonds débités entre le 29 mai et 31 mai 2019, avec intérêts au taux légal à compter du 10 octobre 2019, date de réception du courrier de mise en demeure du 7 octobre 2019 ;

- ordonner l'anatocisme des intérêts au jugement (sic) de l'arrêt ;

- condamner la BNP Paribas à lui payer la somme de 10 000 euros de dommages et intérêts au titre du préjudice moral subi, avec intérêts au taux légal à compter de la délivrance de l'assignation ainsi que la même somme de 10 000 euros de dommages et intérêts au titre de la résistance abusive dont elle a fait preuve à son égard, avec intérêts au taux légal à compter de la délivrance de l'assignation ;

- condamner la BNP Paribas à lui payer la somme de 10 000 euros sur le fondement de l'article 700 du code de procédure civile, avec intérêts au taux légal à compter de la délivrance de l'assignation ;

- condamner la BNP Paribas aux entiers dépens, dont distraction au profit de maître Monique Tardy, avocat, conformément aux dispositions de l'article 699 du code de procédure civile.

La BNP Paribas, dans ses dernières conclusions déposées au greffe et notifiées par RPVA le 19 mai 2022, demande à la cour de :

- confirmer en toutes ses dispositions le jugement ;

- débouter M. [U] de l'intégralité de ses demandes ;

Y ajoutant,

- le condamner à lui verser la somme de 3 000 euros au titre de l'article 700 du code de procédure civile;

- le condamner aux entiers dépens.

L'ordonnance de clôture a été rendue le 3 novembre 2022.

Pour un plus ample exposé des prétentions et des moyens des parties, il est renvoyé à leurs dernières écritures conformément aux dispositions de l'article 455 du code de procédure civile.

SUR CE,

Aucun moyen n'étant soulevé ou susceptible d'être relevé d'office, il convient de déclarer l'appel de M. [U] recevable.

Sur la responsabilité du prestataire de services de paiement :

M. [U] qui agit sur le fondement des articles L.133-18, L.133-19 et L.133-23 du code monétaire et financier et vise également la directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement transposée en droit français par l'ordonnance du 9 août 2017, fait état de la jurisprudence de la Cour de cassation pour rappeler qu'il incombe à la banque de prouver que l'utilisateur du service a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations (Com. 21 novembre 2018, n°17-18.888 et Com. 26 juin 2019, n° 18-12.581), principe régulièrement rappelé par les juridictions du fond.

Il explique avoir été victime des agissements frauduleux d'un tiers qui s'est fait passer au téléphone pour sa conseillère bancaire grâce à une faille de sécurité du système informatique de la BNP, expliquant que le mode opératoire utilisé par les escrocs est fortement répandu et que le 'spoofing' explose dès lors que le canal téléphonique est encore très vulnérable ; il souligne qu'en cas de fraude la banque doit rembourser son client, même si plusieurs banques refusent systématiquement de rembourser leurs clients et ne respectent pas la loi, se référant à la plainte déposée par l'UFC-Que choisir à l'encontre de douze banques dont la BNP Paribas.

Il explique qu'il a été abusé, tout portant à croire à la réception de cet appel que son interlocuteur au téléphone était membre du personnel de la BNP Paribas dès lors que le nom de sa conseillère, dont il avait enregistré le numéro, s'affichait ;qu'il n'a effectué aucun virement et que c'est l'escroc qui a créé les tiers destinataires et procédé aux détournements frauduleux. Il ajoute que ce n'est pas la première fois que la BNP Paribas connaît de graves défauts de son système de sécurité et que compte tenu de la faille de sécurité de la hotline qui a permis l'escroquerie, aucune négligence ne peut lui être reprochée ; il relève qu'il a saisi ses codes personnels non pas par téléphone, email, chat ou sur les réseaux sociaux, comme précisé sur la note de vigilance à la fraude de la banque, mais sur son application ' mes comptes' à la demande de son interlocutrice qui prétendait être l'assistante de sa conseillère habituelle, ce qui l'a nécessairement mis en confiance. Il souligne qu'il a immédiatement informé sa conseillère bancaire dans le respect de l'article L.133-17 du code monétaire et financier et qu'il a porté plainte cinq jours seulement après la survenance des faits.

Il estime qu'en tout état de cause, au regard de la directive UE qui considère que 'la négligence grave devrait impliquer plus que de la simple négligence et comporter un défaut de vigilance caractérisé' et de la jurisprudence nationale, aucune négligence grave ne peut lui être reprochée.

La BNP Paribas fait d'abord état des termes de la plainte déposée par M. [U] pour expliquer 'l'escroquerie' dont celui-ci a été victime, des dispositions de l'article L.133-16 du code monétaire et financier, des consignes de sécurité à respecter qu'elle rappelle régulièrement de même que le gouvernement et les médias et de la jurisprudence de la Cour de cassation dont il ressort que l'appréciation de la 'conscience' attendue de l'utilisateur doit se faire in abstracto, peu important qu'il soit ou non avisé des risques de fraude.

Elle expose ensuite que M. [U] a bien bénéficié du système d'authentification forte exigé par l'ordonnance du 9 août 2017 et que le fraudeur, comme l'a retenu le tribunal, ne pouvait se passer de l'action de validation de M. [U] sur son téléphone mobile pour obtenir l'ajout des cinq bénéficiaires afin de réussir les virements frauduleux, expliquant comment cette opération d'ajout de bénéficiaires de virements a pu être validée par la composition par M. [U] du code

secret qu'il a créé et qu'il est seul à connaître.

L'intimée conteste toute faille de sécurité en précisant que l'appel reçu par M. [U] ne provenait pas de ses services mais de l'escroc se faisant passer pour sa conseillère grâce au procédé du 'spoofing' et que seule la négligence grave de l'appelant dans l'utilisation de son service de paiement a concouru à la fraude puisqu'il a confié à l'escroc ses codes de connexion à son espace sécurisé bancaire de sorte que ce dernier, en possession de ces codes, a créé ces nouveaux bénéficiaires. Elle souligne que M. [U] a ainsi validé à cinq reprises la création des cinq bénéficiaires ce qui a permis au tiers, du fait de son absence de prudence, d'abord de subtiliser ses identifiants confidentiels alors qu'il lui appartenait de prendre toute mesure raisonnable pour en préserver la sécurité puis ensuite de réaliser les virements contestés de sorte qu'elle est déchargée de toute responsabilité. Elle fait à cet égard état de deux jugements de juridiction du fond et d'un arrêt de la Cour de cassation (Com. 1er juillet 2020, 18-21487).

En application de l'article 1937 du code civil, le banquier dépositaire des fonds confiés par son client a l'obligation de ne les restituer qu' à ce dernier ou de suivre ses indications de paiement.

Selon les articles L. 133-16 à L.133-19, L.133-23 et L.133-24 du code monétaire et financier, dans leur rédaction résultant de la transposition par l'ordonnance 2017-1252 du 9 août 2017 de la directive UE 2015/2366 du 25 novembre 2015 relative aux service de paiement, :

- article L. 133-16 :

Dès qu'il reçoit un instrument de paiement, l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés.

Il utilise l'instrument de paiement conformément aux conditions régissant sa délivrance et son utilisation qui doivent être objectives, non discriminatoires et proportionnées ;

- premier alinéa de l'article L.133-17 :

Lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées, l'utilisateur de services de paiement en informe sans tarder, aux fins de blocage de l'instrument, son prestataire ou l'entité désignée par celui-ci ;

- article L. 133-18 :

En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L.133-24, le prestataire de services de paiement du payeur rembourse au payeur le montant de l'opération non autorisée immédiatement après avoir pris connaissance de l'opération ou après en avoir été informé et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, sauf s'il a de bonnes raisons de soupçonner une fraude de l'utilisateur du service de paiement et s'il communique ces raisons par écrit à la Banque de France. Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu (...) ;

- article L. 133-19 :

II. ' La responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées. (...)

IV. ' Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux

obligations mentionnées aux articles L. 133-16 et L. 133-17 (...) ;

- article L. 133-23 :

Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

L'utilisation de l'instrument de paiement telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière. Le prestataire de services de paiement (...) fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement ;

- article L.133-24 :

L'utilisateur de services de paiement signale, sans tarder, à son prestataire de services de paiement une opération de paiement non autorisée ou mal exécutée et au plus tard dans les treize mois suivant la date de débit sous peine de forclusion (....).

La charge de la preuve de la régularité de l'autorisation pèse ainsi sur le prestataire de services de paiement, qui doit établir que l'ordre émane bien de l'utilisateur du service ; c'est aussi au prestataire de services de paiement, soit en l'espèce la BNP Paribas, qu'il incombe de démontrer la négligence grave de son client, étant observé qu'il est jugé que la preuve d'une telle négligence de l'utilisateur d'un service de paiement ne peut se déduire de la seule utilisation effective de son instrument de paiement ou des données personnelles qui lui sont liées et qu'aucune présomption ne doit être attachée à l'infaillibilité supposée des instruments de paiement fortement sécurisés dès lors que le risque de la fraude ne pèse pas sur l'utilisateur.

M. [U], lors de la plainte déposée dès le 3 juin 2019, s'est expliqué en ces termes sur le déroulé des événements ayant conduit aux virements litigieux :

'Mercredi dernier j'ai reçu un appel sur mon téléphone portable qui affichait la BNP Mme [B] [J] qui est ma conseillère. La femme au bout du fil se présente comme l'assistante de Mme [B]. Elle me signale qu'ils ont constaté une attaque de pirate sur mon compte courant. Ils auraient été obligés pour contrer l'attaque de supprimer des bénéficiaires. Elle souhaitait donc qu'on re-valide ces bénéficiaires.

Tout en restant en ligne avec cette femme j'ai reçu des messages toujours émanant de ce numéro de la BNP où figurait à chaque fois de valider les bénéficiaires, qu'effectivement je connaissais. J'ai donc validé à chaque message avec mon code secret. La personne m'a dit ensuite que je n'aurai plus accès à mon compte et que j'allais recevoir par la poste un nouvel identifiant de compte et un nouveau mot de passe. Le vendredi je voulais vérifier que je n'avais plus accès à mon compte et j'ai pu voir l'application de mon téléphone portable en balayant à gauche la position de mon compte qui indiquait un prélèvement d'environ 30 000 euros. J'ai donc tout de suite appelé ma conseillère au même numéro pour lui faire part de la situation. Elle a donc consulté mon compte et a constaté qu'en plus du montant prélevé il y avait aussi des prélèvements à venir pour un montant d'environ 29 000 euros. J'ai donc subi un préjudice total de 59 500 euros (....)'

Sur question de l'agent de police judiciaire, il a précisé qu' 'à la BNP, il n'avait jamais vu ce mode opératoire' ; 'qu'il n'avait jamais vu les messages entrer dans les sms.'

Il est constant que M. [U] a alerté son agence bancaire dès le 31 mai 2019 ; il a précisé dans le compte-rendu des faits effectué par courriel auprès de sa conseillère, transmis le 1er août 2019 au 'Pôle relations clients' de la BNP Paribas, que pour valider les transactions litigieuses présentées comme concernant des bénéficiaires qu'il connaissait, 'la page d'accueil de son application BNP' était 'apparue', lui demandant d'accéder à son compte ; qu'il avait alors entré son code personnel à six chiffres et que les coordonnées d'un de ses bénéficiaires s'étaient affichées à l'écran et qu'il avait validé comme demandé, cela successivement pour '4 à 5 bénéficiaires'. Il précisait dans ce courrier que le 30 mai était le jour de l'Ascension.

La BNP Paribas n'a jamais discuté que M. [U] avait été victime d'une infraction qui a fait l'objet d'un classement sans suite faute pour les services enquêteurs d'avoir pu en identifier les auteurs.

Comme le relève la BNP Paribas, en page 2 de ses écritures, ' les escrocs sont parvenus' à lui faire croire que :

- ' il lui fallait réaliser des opérations d'ajouts de bénéficiaires plutôt que de modifier ses codes d'accès ;

- il lui fallait saisir ses identifiants télématiques confidentiels d'accès à son espace en ligne sur un faux site miroir de la Banque, afin qu'ils soient récupérés.'

L'appelant communique en outre des impressions d'écrans justifiant d'une part qu'il a reçu le 29 mai 2019 sur son téléphone portable plusieurs appels apparaissant sous le nom 'BNP Mme [B] [J]'et que sur son application intitulée 'mes comptes' il a également reçu le même jour cinq demandes de validation de transaction ; sur son relevé de compte figurent cinq opérations débitrices par virements en date du 29 mai 2019, aucun autre virement que les virements litigieux n'apparaissant au débit du compte à cette date.

S'il ressort des déclarations effectuées par M. [U] et du mode opératoire de l'ajout d'un bénéficiaire de virement, tel qu'il est décrit par le guide d'utilisation communiqué par la BNP Paribas, que celui-ci a validé les virements litigieux 'par clé digitale' en validant la notification reçue sur son smartphone à l'aide de son code secret personnel, il n'est pas pour autant caractérisé une négligence grave à son encontre dès lors qu'il croyait être en relation avec une salariée de la BNP Paribas, le numéro d'appel de son interlocutrice apparaissant comme étant celui de sa conseillère dont elle indiquait être l'assistante, et qu'il a cru valider la notification litigieuse sur son application bancaire dont la banque assure qu'il s'agit d'une application sécurisée ; le mode opératoire, par l'utilisation du 'spoofing', soit littéralement une usurpation d'identité, a mis M. [U] en confiance et a diminué sa vigilance, étant observé que face à un appel téléphonique évoquant de surcroît un piratage, la vigilance de la personne qui reçoit cet appel est moindre que celle d'une personne qui réceptionne un mail, laquelle dispose de davantage de temps pour en prendre connaissance et s'apercevoir d'éventuelles anomalies révélatrices de son origine frauduleuse.

En outre M. [U] n'a aucunement tardé dans la révélation de ces virements frauduleux à sa banque.

Dans ces circonstances, quand bien même M. [U] a fait usage de son code confidentiel, étant observé qu'il n'est pas démontré qu'il l'a communiqué par téléphone, email, chat ou sur les réseaux sociaux comme le mettait en garde la BNP Paribas mais qu'il a indiqué l'avoir saisi sur son application, il n'est pas caractérisé à son égard une négligence grave.

La banque est donc tenue de restituer les fonds correspondant aux virements litigieux, seul l'un deux ayant pu être bloqué et recrédité sur le compte de M. [U] le 3 juin 2019.

Sur les demandes chiffrées de M. [U] :

Outre le paiement de la somme débitée sur son compte entre les 29 et 31 mai 2019 avec intérêts au taux légal à compter de la mise en demeure adressée par son conseil le 10 octobre 2019 à la BNP Paribas, M. [U] sollicite la condamnation de cette dernière à lui verser la somme de 10 000 euros en réparation du préjudice moral et du 'stress post-traumatique très important' qu'il soutient subir depuis ces événements dont il affirme qu'ils l'ont particulièrement affecté, d'autant plus au regard du défaut d'assistance de l'intimée tant avant que pendant et après la survenance des faits litigieux et de son accusation d'une négligence grave alors qu'il est client depuis plus de 45 ans de celle-ci. Il prétend également qu'elle fait preuve de mauvaise foi en persistant à ignorer ses obligations contractuelles d'indemnisation du préjudice financier qu'il a subi alors qu'elle a pleinement conscience du caractère contestable des virements effectués qu'elle a pu bloquer pour l'un d'entre eux.

La BNP Paribas conclut au débouté de toutes les demandes de M. [U] au regard de sa négligence grave.

Le quantum des virements contestés par M. [U], lesquels sont mentionnés sur son relevé de compte, n'est pas discuté par la BNP Paribas ; il convient, infirmant le jugement, de la condamner au paiement de la somme de 54 500 euros avec intérêts au taux légal à compter du 10 octobre 2019, la mise en demeure adressée à la BNP Paribas étant datée du 7 octobre 2019 et celle-ci ne contestant pas le point de départ de ces intérêts.

Conformément à la demande de M. [U] et aux dispositions de l'article 1343-2 du code civil, la capitalisation des intérêts échus, dus au moins pour une année entière, sera ordonnée.

Il n'est pas contestable que M. [U], client depuis de nombreuses années de la BNP Paribas, ce que celle-ci ne conteste pas, a été moralement affecté par le refus de remboursement qu'elle lui a opposé au prétexte d'une négligence grave qu'elle ne démontre pas, étant observé que celle-ci n'a jamais mis en doute l'existence de l'infraction dont il l'a alertée très rapidement ; son préjudice moral sera justement réparé par l'allocation de la somme de 1 500 euros, l'appelant n'apportant aucun élément pour démontrer l'important stress post-traumatique dont il fait état et ne pouvant faire supporter à la banque le préjudice qui résulte de l'infraction dont il a été victime et qui est imputable à un tiers qui n'a pu être identifié.

S'agissant d'une condamnation indemnitaire, la BNP Paribas sera condamnée au paiement de cette somme avec intérêts au taux légal, non pas à compter de l'assignation mais à compter du présent arrêt, conformément aux dispositions de l'article 1231-7 du code civil.

Le tribunal a débouté M. [U] de l'intégralité de ses prétentions en accueillant l'argumentation de la BNP Paribas de sorte qu'il ne peut être considéré que celle-ci a fait preuve d'une résistance abusive en refusant de procéder au remboursement de la somme de 54 500 euros ; par conséquent, il convient de confirmer le jugement en ce qu'il a débouté M. [U] de sa demande de dommages et intérêts au titre de la résistance abusive.

PAR CES MOTIFS

Statuant par arrêt contradictoire,

Déclare l'appel de M. [Y] [U] recevable ;

Infirme le jugement du 3 novembre 2021 sauf en ce qu'il a débouté M. [Y] [U] de sa demande de dommages et intérêts au titre de la résistance abusive ;

Condamne la société BNP Paribas à verser à M. [Y] [U] la somme de 54 500 euros avec intérêts au taux légal à compter du 10 octobre 2019 ainsi que la somme de 1 500 euros à titre de dommages et intérêts pour préjudice moral avec intérêts au taux légal à compter du présent arrêt ;

Ordonne la capitalisation des intérêts échus, dus au moins pour une année entière ;

Condamne la société BNP Paribas à verser à M. [Y] [U] la somme de 6 000 euros en application des dispositions de l'article 700 du code de procédure civile ;

Condamne la société BNP Paribas aux dépens de première instance et d'appel qui seront recouvrés par maître Monique Tardy conformément aux dispositions de l'article 699 du code de procédure civile.

Prononcé publiquement par mise à disposition de l'arrêt au greffe de la cour, les parties en ayant été préalablement avisées dans les conditions prévues au deuxième alinéa de l'article 450 du code de procédure civile.

Signé par Madame Marie-Andrée BAUMANN, Conseiller faisant fonction de Président, et par Madame Sabine NOLIN, Greffier, auquel la minute de la décision a été remise par le magistrat signataire.

Le Greffier, Le Conseiller faisant fonction de Président,

28 mars 2023